

ClearPass Onboard Overview

Seth Fiermonti
Consulting Systems Engineer Northeast
@sethfiermonti



What is a Certificate

Sometimes called a public key

What is a Certificate?



PUBLIC
KEY



METADATA

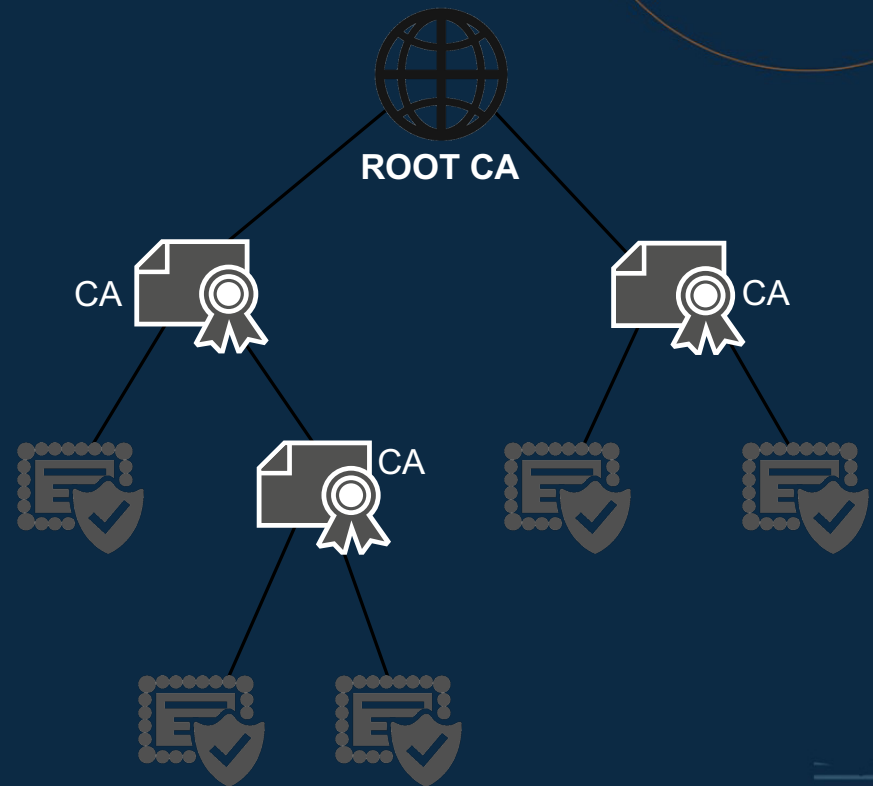
Methods of Certification

- Certificate Authorities
 - A 3rd party will digitally sign the public key
 - Other people/systems who trust the CA can then trust you are who you claim
 - Need to be able to interact with something to determine if the trust is still valid
 - This is how most people use the web
- Simple PKI
 - Parties directly exchange their public keys, no need for additional trust points
 - Manually need to maintain trust information
 - This is how some SSH and “passwordless authentication” use cases work
- We are only discussing Certificate Authority methods today

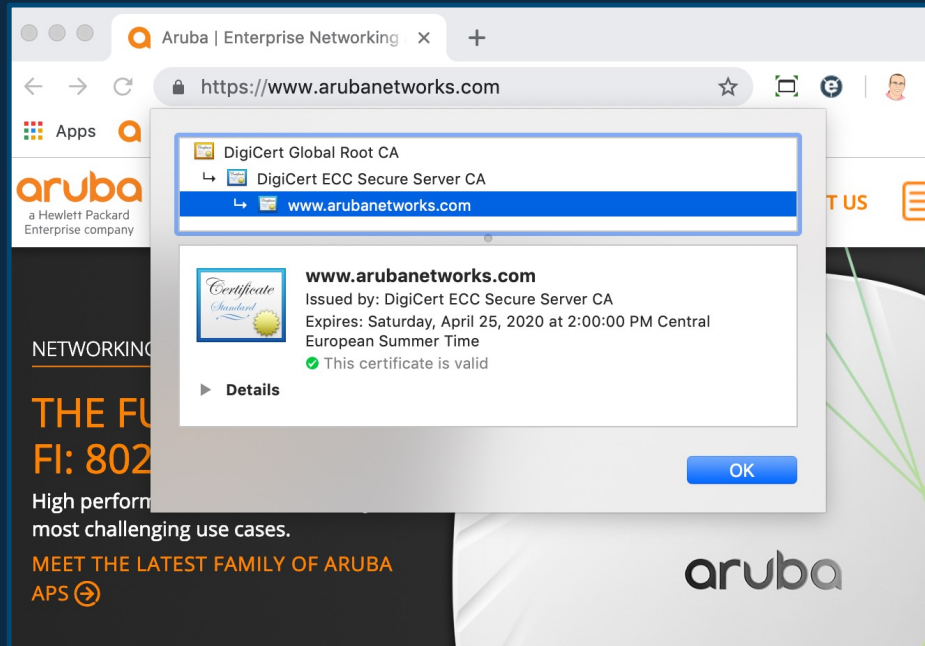


It's all about trust!

- A Certificate Authority (CA) guarantees the binder between a public key and another CA or an End Entity (EE)
- Each device has a trusted CA store
- Some organizations have an issuing CA off a commercial root



Example – <https://www.arubanetworks.com>



DigiCert Global Root CA

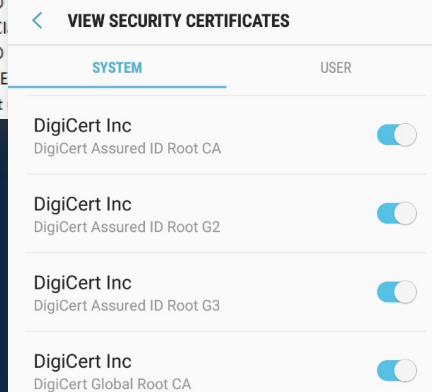
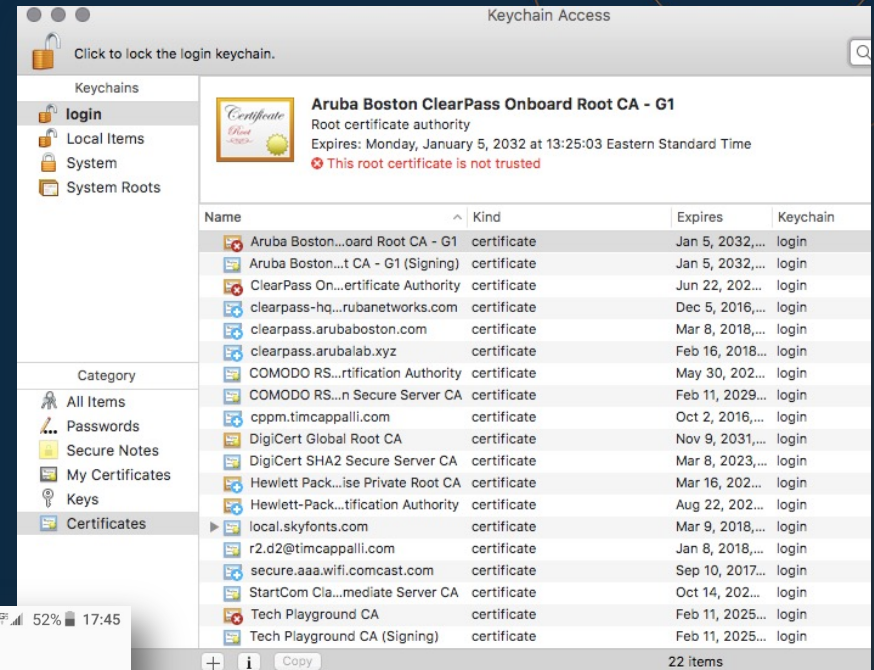
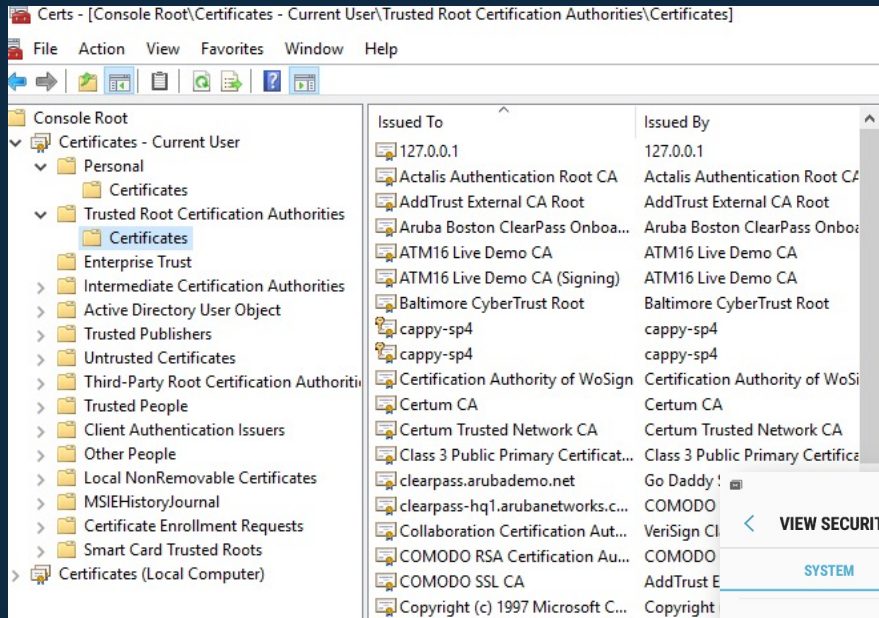


DigiCert SHA2 Secure Server CA

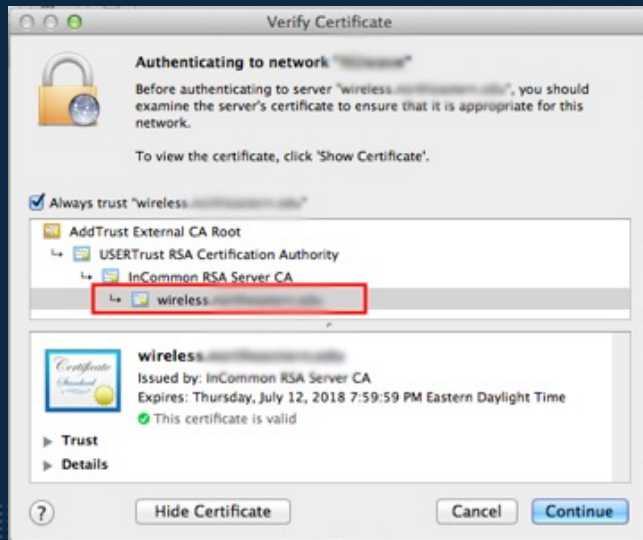


DNS: www.arubanetworks.com

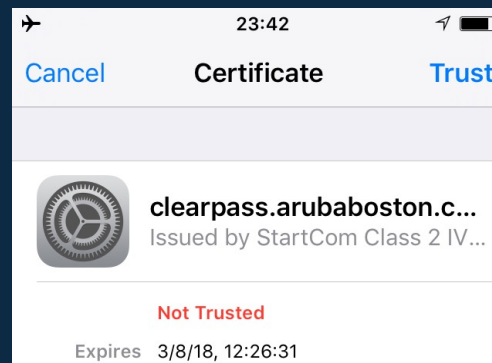
Certificate Stores



"The Error"



THIS IS
NORMAL!*



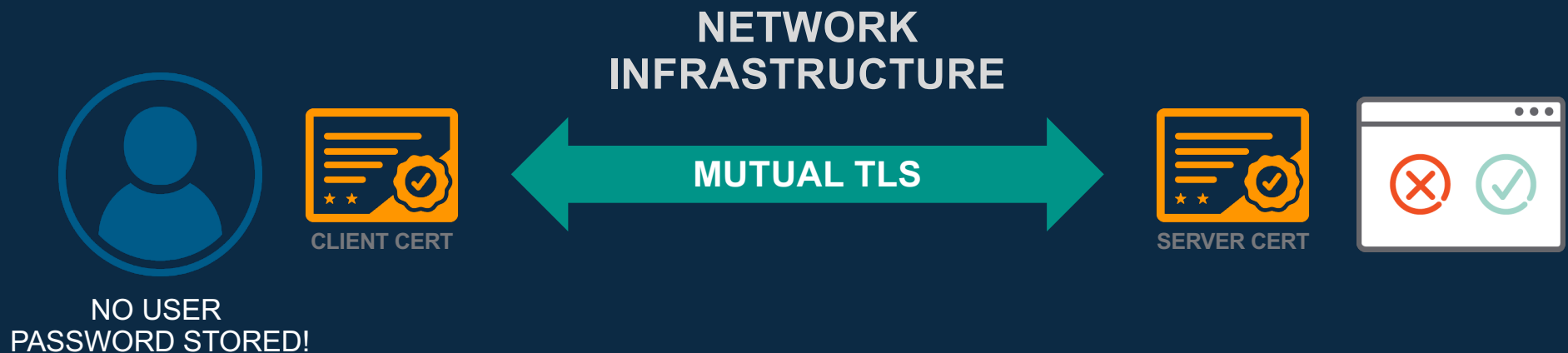
* on unconfigured devices



What Uses Certificates?

- EAP/RADIUS
- RadSec (RADIUS over TLS)
- HTTPS
- SMTP (sometimes)
- Database communications
- VPNs
- ClearPass servers
- Supplicants
 - EAP-TLS
- Controllers
- Switches
- Administrators
 - Mutual authentication HTTPS

EAP-TLS



- Credentials are not stored locally on the device
- Gives the device a unique identity
- Flexible certificate properties
- Device properties stored in certificate

EAP-TLS Certificates Need to be Valid



Trusted Issuer



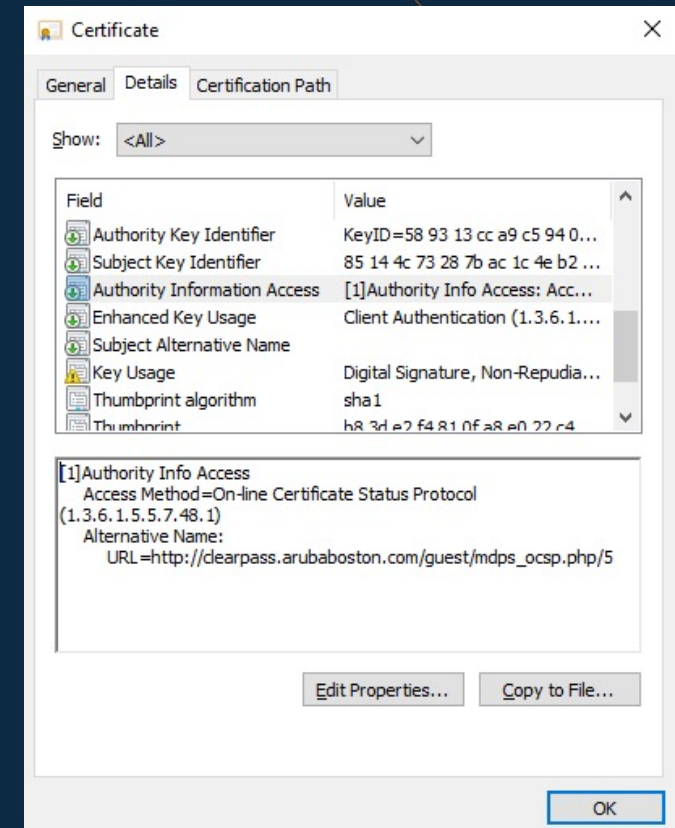
Not Expired



Not Revoked

OCSP – Is my certificate still valid

- Online Certificate Status Protocol
 - Runs over HTTP
 - Real-time check
- EAP-TLS method in ClearPass controls OCSP check for the authentication request
- Pay attention to OCSP URL for Onboard
 - Single cluster vs multi cluster
 - Multiple uses
 - Multiple CAs



Sample OCSF Response

OCSP Request Data:

Version: 1 (0x0)

Requestor List:

Certificate ID:

Hash Algorithm: sha1

Issuer Name Hash: 939E0296797407B76FB212BB47BAB99DEDF8C102

Issuer Key Hash: F6E04582CB0C4B0EB4588821F58E47BE24866050

Serial Number: 1425DCA4CC5BC2AF83A0F2D3ADE8DD20

Request Extensions:

OCSP Nonce:

0410A944392A4A496241BCA5679CB96DBF01

OCSP Response Data:

OCSP Response Status: successful (0x0)

Response Type: Basic OCSP Response

Version: 1 (0x0)

Responder Id: 645ABF4B99FDD84F7BE780014528059C6562E681

Produced At: Feb 16 08:58:07 2017 GMT

Responses:

Certificate ID:

Hash Algorithm: sha1

Issuer Name Hash: 939E0296797407B76FB212BB47BAB99DEDF8C102

Issuer Key Hash: F6E04582CB0C4B0EB4588821F58E47BE24866050

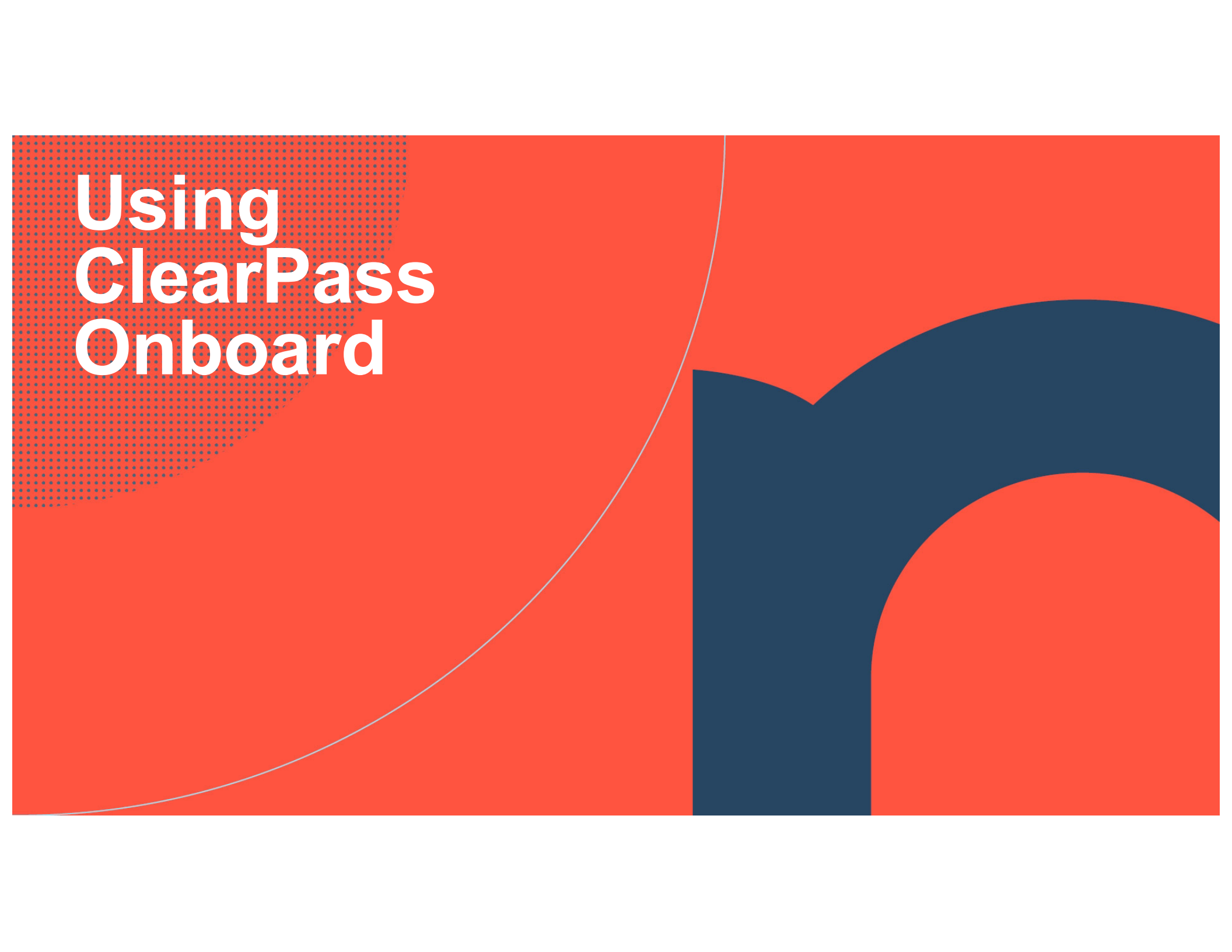
Serial Number: 1425DCA4CC5BC2AF83A0F2D3ADE8DD20

Cert Status: good

This Update: Feb 16 08:58:07 2017 GMT

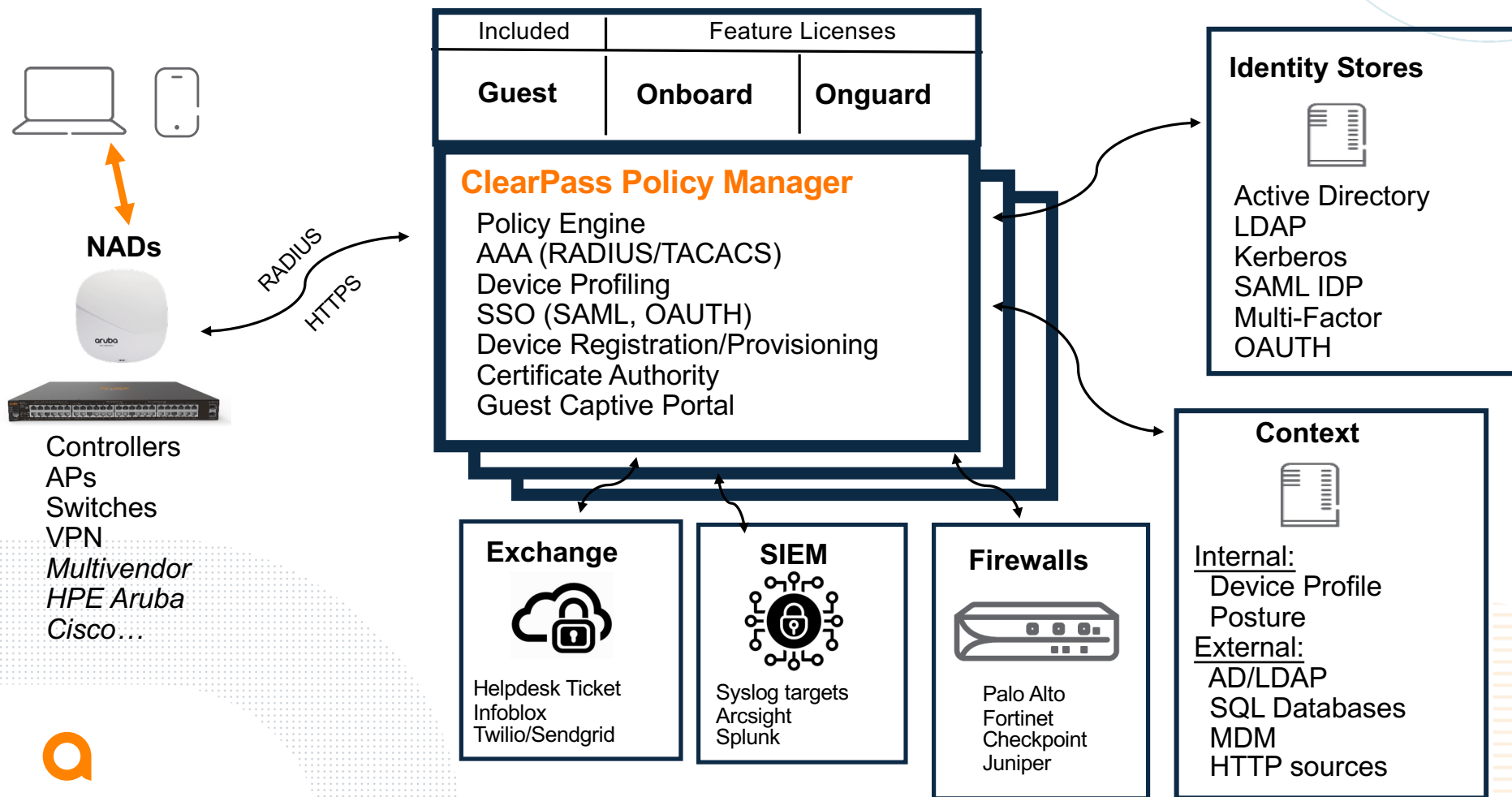
PROPRIETARY UNRELEASED INFORMATION





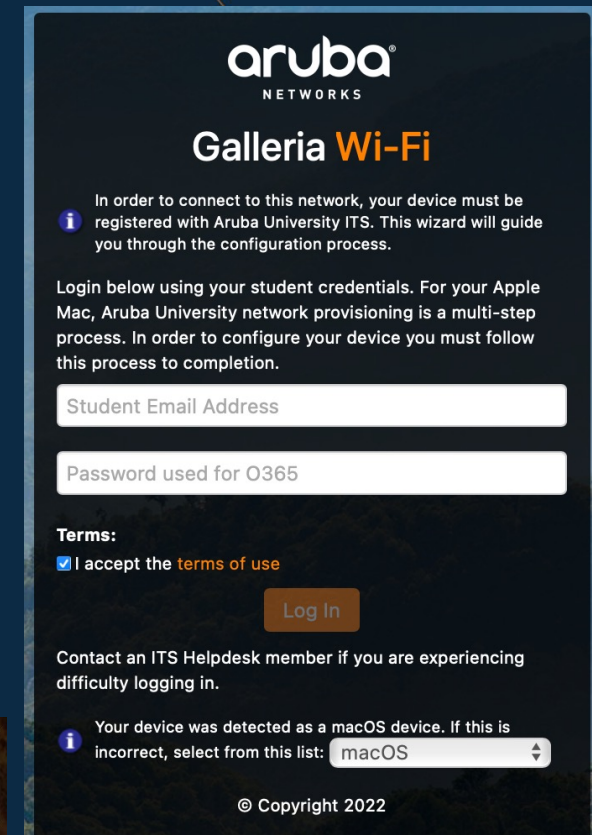
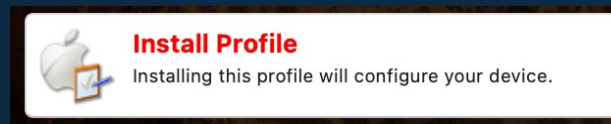
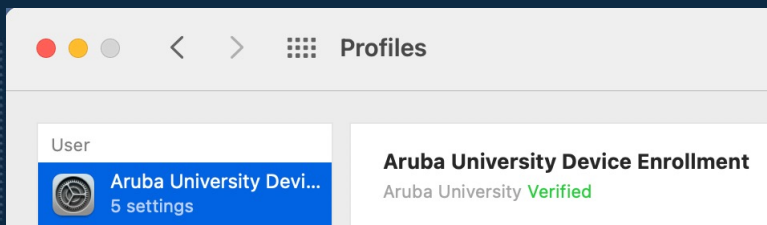
Using ClearPass Onboard

ClearPass Recap



What is ClearPass Onboard

- Automatic configuration of network settings for wired and wireless endpoints
- Provisioning of unique device credentials for BYOD and IT-managed devices
- Support for Windows, macOS, iOS, iPadOS, and Android devices
- Ability to revoke unique credentials on a specific user's device
- Set limits using context from identity stores
- ClearPass Profiler for identifying device type, manufacturer, and model
- Support for 1:1 user to device or many users to a shared device
- Self-service portal to manage enrollment and device lifecycle



ClearPass Onboard Methods

Device vs. User Registration

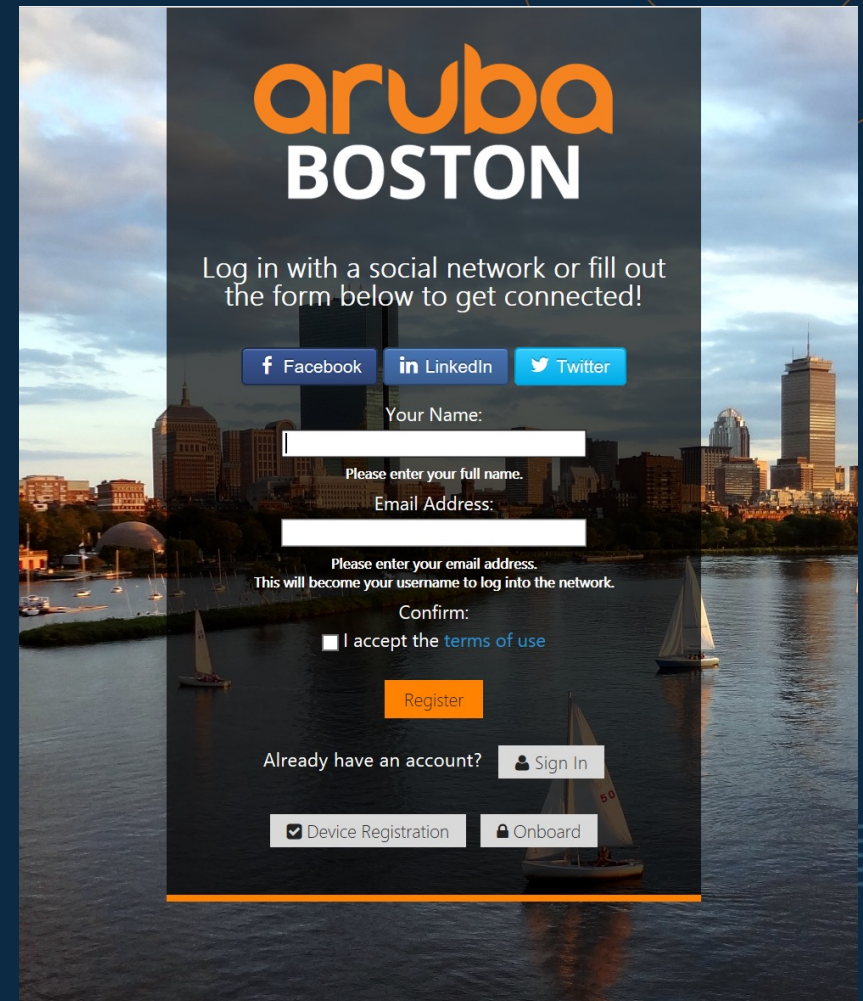
–ClearPass offers two options

1. Device Enrollment and unique credential provisioning – EAP-TLS certificates with policy
 - Eduroam onboarding
 - Unique certificate per user per device (provisions for shared systems)
 - Highest security
 - Requires Onboard license or subscription
2. “Headless device” registration – mac address based self-service entry with policy
 - Game systems, smart TVs, IOT devices, etc
 - mPSK option available with Aruba WLAN – unique PSK per MAC address
 - Included in ClearPass base license

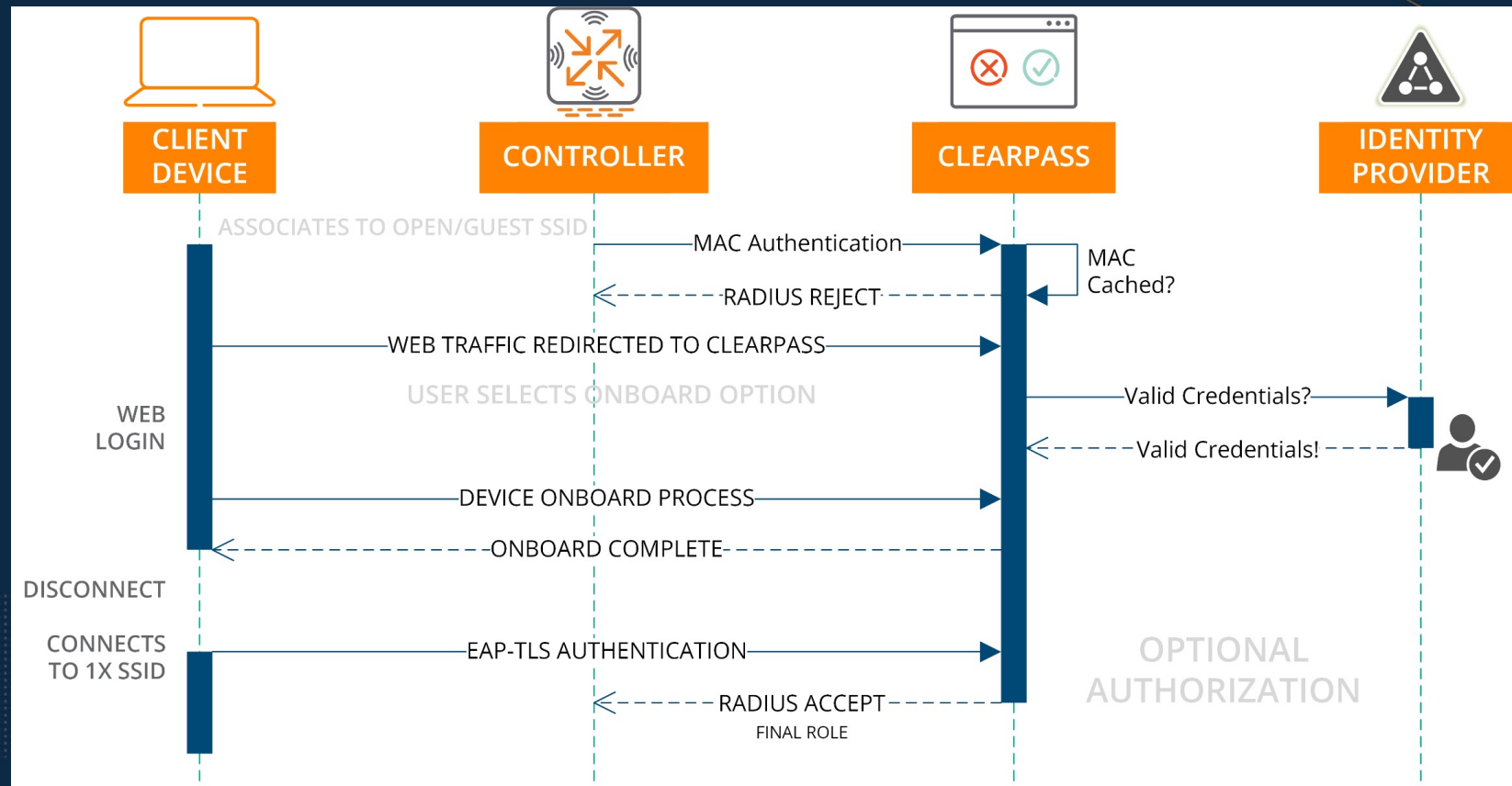


Leverage your guest network!

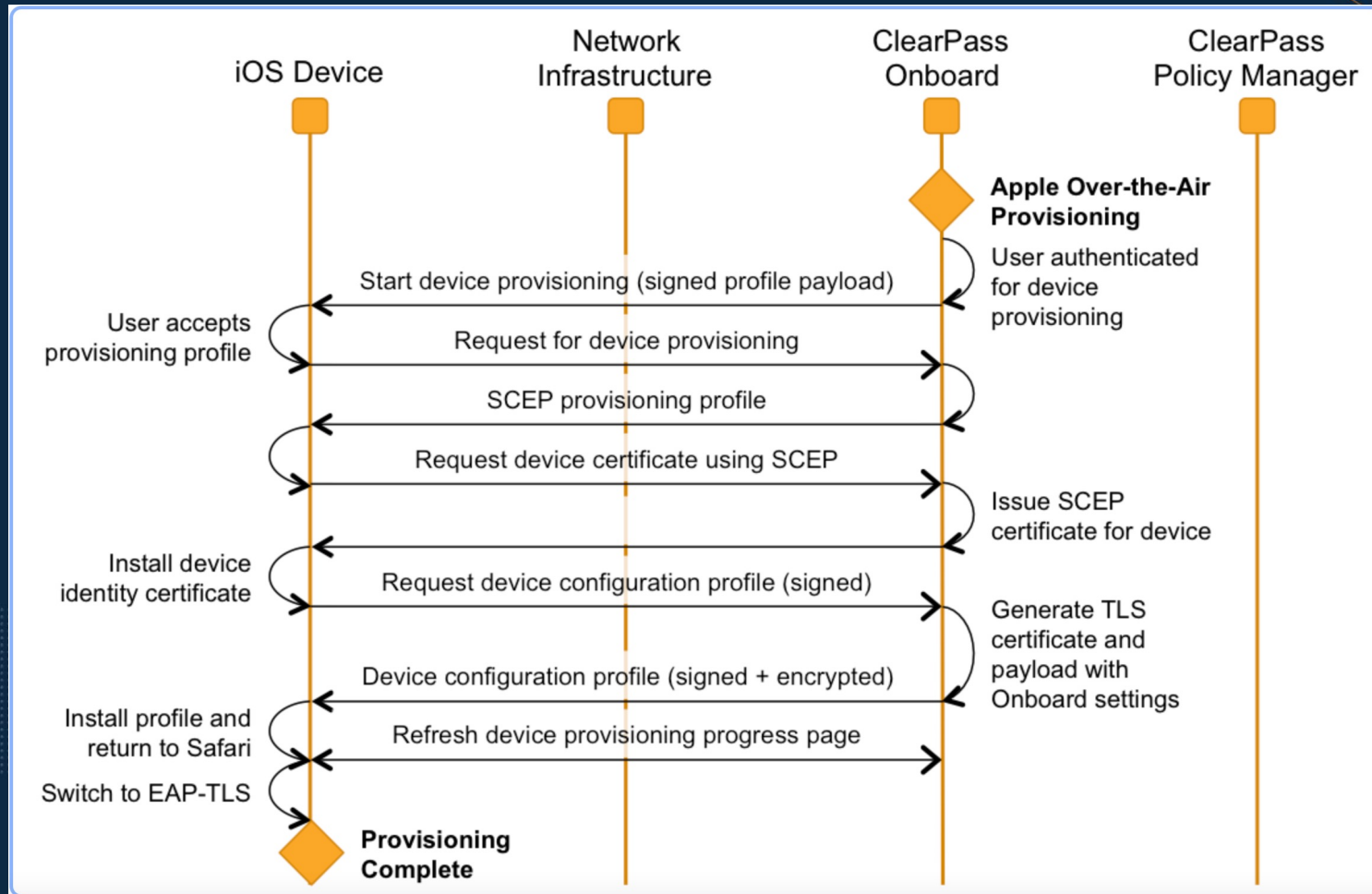
- You don't need a dedicated SSID for Onboarding!
- Use your guest network. It's already there!
- Additional SSIDs add overhead and confusion
- Leverage SAML or OAuth 2.0
 - Microsoft Azure MFA
 - DUO
 - Other SSOs like OKTA

The image shows a web-based onboarding interface for the 'aruba BOSTON' guest network. The background is a scenic view of the Boston skyline at dusk, with sailboats on the water. The interface is centered and features the Aruba logo in orange and 'BOSTON' in white. Below the logo, it prompts users to 'Log in with a social network or fill out the form below to get connected!'. There are three buttons for social login: Facebook, LinkedIn, and Twitter. Below these are input fields for 'Your Name:' and 'Email Address:', each with a placeholder text: 'Please enter your full name.' and 'Please enter your email address. This will become your username to log into the network.' respectively. A 'Confirm:' section has a checkbox for 'I accept the terms of use'. An orange 'Register' button is positioned below the terms. At the bottom, there's a 'Sign In' button for users with accounts, and two checkboxes for 'Device Registration' and 'Onboard'.

ClearPass Onboarding Workflow using Guest SSID






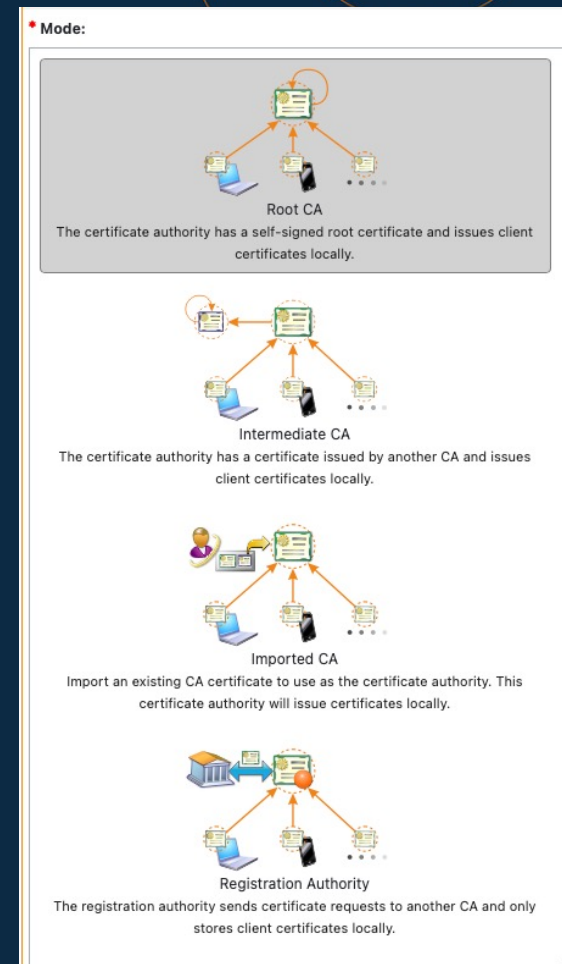
ClearPass Onboarding Process with iOS



ClearPass Onboard Configuration Encompassing PKI options

- Support for multiple certificate authorities
 - Useful for segmentation of larger user/device bases
 - Different CA properties
- Use existing PKI already in production
- Create different expiration periods
 - students vs lab machines
- Option for ADACS integration or proxy to a reg authority















Name	Mode	Status	Expiry	OCSP URL
 BC Onboarding CA	root	✓ Valid	2032-01-28T15:57:52-05:00	http://clearpass.fiermonti.net/onboard/mdps_ocsp.php/5
 Fiermonti CA	root	✓ Valid	2024-12-21T11:36:35-05:00	http://clearpass.fiermonti.net/onboard/mdps_ocsp.php/2
 Gonzaga Onboarding CA	root	✓ Valid	2032-01-28T19:24:17-05:00	http://clearpass.fiermonti.net/onboard/mdps_ocsp.php/6
Showing 1 – 3 of 3				
Refresh 1 20 rows per page				



ClearPass Onboard Configuration

Multiple options and use cases

- Support for multiple provisioning profiles
- Create profiles for wired, wireless, or both
- Only allow certain OS types to onboard
- Restrict only certain groups based on AD

Name	Network Type	SSID
 eduroam - LAB Settings to allow shared lab machines with multiple user logins	 Wireless	eduroam
 eduroam - user Network SSID settings for user authentication	 Wireless	eduroam
 Fiermonti-Secure SSID Connect to the fiermonti-secure network.	 Wireless	fiermonti-secure
 Gonzaga Community - LAB Settings to allow shared lab machines with multiple user logins	 Wireless	Gonzaga Community
 Gonzaga Community - user Network SSID settings for user authentication	 Wireless	Gonzaga Community
 Gonzaga Community - wired and wireless Profile to configure authentication on specified SSID as well as the wired NIC	 Both	Gonzaga Community
 Wired Authentication - user Profile for provisioning certificate network access for a wired edge port applying to user authentication	 Wired	

General
Supported Devices
Web Login
Instructions & Messages
Apple Profiles
Onboard Client
Sponsorship Confirmation

Device Provisioning Settings

Android Provisioning

These options control Android device provisioning.

Android Devices:

☒ Enable Android device provisioning
Downloads and executes an Android application on a user's device to complete provisioning.

Android Rootkit Detection:

Do not provision rooted devices
Control whether devices with a rootkit may be provisioned.

Android Browser Check:

☐ Enable browser checking for Android
Force Android users to provision using the default (ie Chrome) browser.

Chrome OS Provisioning

These options control Chrome OS device provisioning.

Chrome OS Devices:

☐ Enable Chrome OS device provisioning
Provides a certificate to Chrome OS devices. Requires the device to be under management and the QuickConnect extension to be configured for pre-install.

iOS Provisioning

These options control iOS device provisioning.

iOS Devices:

☒ Enable iOS device provisioning
Provision iOS devices via Apple's 'Over-the-Air' profile delivery process.

iOS Browser Check:

☒ Enable browser checking for iOS
Force iOS users to provision using the default (ie Safari) browser.

iPadOS Provisioning

These options control iPadOS device provisioning.

iPadOS Devices:

☒ Enable iPadOS device provisioning
Provision iPadOS devices via Apple's 'Over-the-Air' profile delivery process.

iPadOS Browser Check:

☒ Enable browser checking for iPadOS
Force iPadOS users to provision using the default (ie Safari) browser.

macOS Provisioning

These options control macOS device provisioning.

macOS Devices:

☒ Enable macOS 10.7+ (Lion or later) device provisioning
Provision macOS 10.7+ (Lion or later) devices via Apple's 'Over-the-Air' profile delivery process.

ClearPass Onboard Configuration

Customizable user facing pages

- Full control over web page look and feel
- Customize labels, forms, HTTP/CSS code
- Use Aruba's skins service to match current branding and web design style
- Several options to override default labels and values

Web Login Page

Options for the weblogin landing page for Onboard.

* Page Name:

Enter a page name for this web login.

The web login will be accessible from "/onboard/page_name.php".

Login Page

Options for controlling the look and feel of the login page.

* Skin:

Choose the skin to use when this web login page is displayed.

Title:

The title to display on the web login page.

Leave blank to use the default (Register Your Device).

Header HTML:

```
{nwa_icontext type=info}
  {nwa_text id=16344}In order to connect to this network, your
  device must be registered with Aruba University ITS. This wizard
  will guide you through the configuration process.{/nwa_text}
{/nwa_icontext}

{capture assign=organization_name}{nwa_mdps_config
name=organization_name}{/capture}
{nwa_text id=14462 1=$organization_name|escape}Login below
using your student credentials.{/nwa_text}

{onboard_device_message}
```

HTML template code displayed before the login form.

Footer HTML:

```
{nwa_text id=7979}<p>
Contact an ITS Helpdesk member if you are experiencing
difficulty logging in.
</p>{/nwa_text}
```



ClearPass Onboard Configuration

Integrate with cloud identity and MFA

- Support MFA and cloud identity
- Based on provisioning profile – not “all or nothing”
- Several cloud and social identity sources to choose from

Multi-Factor Authentication

Require a secondary factor when authenticating.


Provider:

- ✓ No multi-factor authentication
- Duo Security – Two Factor Authentication
- ImageWare Systems – Solutions Powered by GoVerifyID
- SMS Verification Codes


Cloud Identity
Optionally present guests with various cloud identity / social login options.

Enabled:
☒ Enable logins with cloud identity / social network credentials

Authentication Providers:

 Add new authentication provider

Use the form below to add an authentication provider to this login.

 Cloud identity allowlists for use in captive portals

Properties

* **Provider:** Microsoft Azure AD

Enabled: ☒ Use this provider

* **Client ID:** e783297329132132hnjkhjkhjk
The Client ID associated to your provider. They may use a different label.

* **Client Secret:** djskrh3kjh4k3nmweiwojekwqnmenqw
The Client Secret associated to your provider. They may use a different label.



Advanced: ☐ Show advanced properties

Endpoint Attributes: Do not store any user data
Creating attributes is only needed if you are creating specialized enforcement policies on them. Attributes may include publicly identifiable information (PII). Refer to local laws and regulations how this data must be treated.

VIP Attribute: userType
Enter the name of the user record attribute to apply to the "social_vip" flag. Refer to the Microsoft Graph API for retrieving users.

Group Membership: ☒ Retrieve the group memberships for the guest's account

Tenant:
To redirect directly to your Azure AD tenant, add your tenant ID (GUID) or tenant realm (domain). Other supported values: 'common' (default), 'organizations' and 'consumers'.

 Add  Cancel



ClearPass Onboard Lifecycle Management

Certificate expirations and inactivity

- Proactively notify users
- Optionally send to a default mailbox
- Customize the email format and content
- Expire/revoke certificates based on inactivity

Revoke Inactive:

☒ Revoke certificates for inactive devices
If checked the certificates for devices will be revoked after a period where the device is not seen on the network.

Information: This feature relies on data from ClearPass Insight. You must have a primary Insight node enabled and with an appropriate data retention period configured for inactivity calculations to work correctly.

*** Inactivity Period:**

30 days
If a device does not authenticate on the network after this period its certificate will be revoked.

Certificate Expiry:

☒ Notify users before their device credentials expire
If checked users will receive an email notification when their device's network credentials are due to expire.

* Send Email Notification:

4 weeks prior to expiration
Select the time to send an email notification.

* If Email is Unknown:

Send a message to a fixed email address
Specify where to send emails to if the user's certificate doesn't have an email address recorded.

* Unknown Address:

onboard_expiration@arubauniversity.edu
Address used when no email address is known for a user.

Subject Line:

Your network credentials are about to expire
Enter a subject for the notification email.
Leave blank to use the default (Your network credentials are about to expire).



ClearPass Onboard Lifecycle Management

Management of certificates

- View by device, user, or certificate
- Revoke or delete user's device
- Enable self-service for a user or department
- Obtain device details

The screenshot shows the 'Manage Access' section for a macOS device. At the top, it displays the device type (macOS), user (Seth's MacBook Air), and device ID (udid:222798A9-999C-5B0D-8AEC-B569A353D86E). Below this, there are navigation links: 'Show Config', 'Device Details', 'Show Users', 'Manage Access', and 'Device Actions'. A message states: 'Use this form to control a device's access to the network.' The 'Manage Access' section has a dropdown menu set to 'Deny access to this device'. Below the dropdown, it says 'Access: Control whether this device will be able to enroll and access the network.'

Device Type	Device Name	Device ID	User	Status	Onboarded	Managed By
macOS	Seth's MacBook Air	udid:222798A9-999C-5B0D-8AEC-B569A353D86E	seth	Enrolled	✓ 1 User(s)	
macOS	Seth's MacBook Pro	udid:EAF704D9-FB6C-556B-A394-1BDBBB97EC09	seth	Enrolled	✓ 2 User(s)	
iOS	iOS	udid:00008101-0004786E3688001E	seth	Enrolled	✓ 1 User(s)	
iPadOS	iPadOS	udid:00008027-001224622262802E	seth	Enrolled	✓ 1 User(s)	
Windows	Windows 10	mac:ac:82:47:4b:10:9a	seth	Enrolled	✓ 1 User(s)	





Configuring ClearPass Onboard

ClearPass Onboard Checklist

1. Configure the Onboard Certificate Authority.
2. Configure network settings for device provisioning.
 - Set network properties – SSID name, authentication method/type
 - Set device-specific networking settings
3. Bind network settings to configuration profile
4. Configure the Onboard provisioning settings
 - Select certificate options for device provisioning
 - Select the configuration profile
 - Select which device types should be supported
 - Setup and customize the device provisioning web login page
 - Customize text for labels and messages shown before, during, and after provisioning
 - Specify options for Apple device provisioning and security
 - Customize the Onboard client for Windows and Android
 - Enable sponsorship (optional)
5. Create the Policy Manager Services



ClearPass Onboard Suggestions

- ✓ Use the ClearPass Onboard Certificate Authority
 - Consider multiple CAs for different groups or functional purposes
- ✓ Use a publicly signed certificate as the code-signing cert
 - Streamlines the user experience specifically for Apple devices
 - Eliminates the root certificate download step
- ✓ Use the dual-SSID method
 - Consider the guest network or a dedicated provisioning SSID
- ✓ Customize available instructions, settings, web content
 - Provide self-help and guidance along the way



1. Create a New Certificate Authority

- Choose Root CA
- Set a user friendly name indicating intent of the CA.
 - Example: Aruba University Device Enrollment CA
 - Enter an institution specific email address
- Private Key type should be at least 2048-bit
- Expiration of the CA should be lengthy
 - NOTE: This is not the expiration time of the onboarded certificates

* CA Expiration:

3653 days

The number of days before the certificate authority's root certificate will expire.

* Mode:



Root CA

The certificate authority has a self-signed root certificate and issues client certificates locally.

* Common Name:

ClearPass Onboard Local Certificate Authority

Enter a name for the certificate authority. This is the 'common name' of the digital certificate.

* Signing Common Name:

ClearPass Onboard Local Certificate Authority (Sig

Enter a name for the signing certificate. This is the 'common name' of the digital certificate.

Email Address:

d69be3b5-4e37-4cb5-9f19-f3e76f0b0c4f@exam

Enter an email address.



2. Configure Onboard Network Settings

- *Access tab*
- Create a friendly name
- Set network type to wireless
- Set security type to 802.1X
- Enable checkbox to automatically connect

Network Settings » Network Access

Access Protocols Authentication Trust Windows Proxy

Network Access
Options for basic network access.

* **Name:**
Aruba University Secure SSID
Enter a name for the network.

Description:

Enter a description for the network.

* **Network Type:**
Wireless only
Select which types of network will be provisioned.
Enterprise security (802.1X) will be selected if wired networks are to be supported.

* **Security Type:**
Enterprise (802.1X)
Select the authentication method used for the network.
Enterprise security (802.1X) will be selected if wired networks are to be supported.

Wireless Network Settings
Options for wireless network access.

* **Security Version:**
WPA2 with AES (recommended)
Select the WPA encryption version for the wireless network.
This setting is used for Windows, Android and Legacy OS X (10.5/6) devices only.
iOS and macOS 10.7+ (Lion or later) devices auto-detect the WPA version.

* **SSID:**
Aruba University Secure
Enter the SSID of the wireless network to connect to.

Wireless:
☐ Hidden network
Select this option if the wireless network is not open or broadcasting.

Auto Join:
☒ Automatically join network
Select this option to automatically join the wireless network.

Next Save Changes Cancel

2. Configure Onboard Network Settings

– On the *Protocols* tab, leave all defaults to TLS

Use this form to create the network settings that will be sent to a provisioned device. [Help](#)

Network Settings » Enterprise Protocols

[Access#](#) [Protocols](#) [Authentication](#) [Trust](#) [Windows](#) [Proxy](#)

Enterprise Protocols
Options for 802.1X protocols supported on the network.

iOS & macOS EAP

iOS & macOS EAP:

Accepted EAP Types

☒ TLS ☐ PEAP ☐ EAP-SIM
☐ TTLS ☐ EAP-FAST
Select the authentication protocols to use when configuring an iOS or macOS 10.7+ (Lion or later) device.

Legacy OS X EAP

Legacy OS X EAP:
PEAP with MSCHAPv2
Select the authentication protocol to use when configuring OS X 10.5/6 (Leopard/Snow Leopard) devices.

Android EAP

Android EAP:
TLS
Select the authentication protocol to use when configuring an Android device.

Windows EAP

Windows EAP:
TLS
Select the authentication protocol to use when configuring a Windows device.

Ubuntu EAP

Ubuntu EAP:
TLS
Select the authentication protocol to use when configuring an Ubuntu device.

[Previous](#) [Next](#) [Save Changes](#) [Cancel](#)



2. Configure Onboard Network Settings

- On the *Authentication* tab, leave all defaults for 1:1 user to device enrollment

Use this form to create the network settings that will be sent to a provisioned device. [? Help](#)

Network Settings » Enterprise Authentication

[Access#](#) [Protocols](#) [Authentication](#) [Trust](#) [Windows](#) [Proxy](#)

Enterprise Authentication

Options for 802.1X authentication used on the network.

Android Authentication

*** Certificate Store:**

Private

Select the certificate store where the client certificate will be provisioned when configuring an Android device. Installing to the system store will make certificates available for use by other applications, but may require additional security prompts during provisioning.

iOS & macOS Authentication

*** iOS & macOS Credentials:**

Certificate

Select the type of credentials to provision for iOS and macOS 10.7+ (Lion or later) devices.

Windows Authentication

*** Certificate Store:**

User

Select the certificate store where the client certificate will be provisioned when configuring a Windows device.

[Previous](#) [Next](#) [Save Changes](#) [Cancel](#)

2. Configure Onboard Network Settings

- On the *Trust* tab, leave the default settings

- Change these settings to push additional or different RADIUS server certificates to the device for trust purposes
 - Example: ADACS workflow or non ClearPass authentication servers
- Remaining tabs - Windows and Proxy - leave at default settings

Enterprise Trust

Certificate trust options for 802.1X protocols supported on the network.

Configure Trusted Servers:

Automatically configure trusted servers (recommended) ▾

Automatic settings will trust all ClearPass servers currently in the cluster.

You should manually enter server names if:

- You are not using ClearPass for RADIUS authentication
- You plan to expand your ClearPass cluster at a later date (use a wildcard rule in this case)

Configure Trust:

Automatically configure trust settings (recommended) ▾

Use automatic configuration if you are using Policy Manager for authentication. Otherwise, select manual configuration.

3. Configure Onboard Configuration Profile

- The purpose of the Configuration Profile is to bind the Network Settings from step 2
- It is possible to provision multiple networks (SSIDs) to the enrolled devices in a single Configuration Profile
- For this walkthrough, only select the network defined in the previous step

Networks:

- ☒ Aruba University Secure SSID
- ☐ eduroam - LAB
- ☐ eduroam - user
- ☐ Fiermonti-Secure SSID

4. Configure Onboard Provisioning Settings

Putting it all together – General tab

- Give the entire profile a friendly name and description
- Enter the Organization's name
- Under Identity, select the CA configured in Step 1
- Under Authorization, leave the default App Authentication. We will configure this next in a Policy Manager service
- Select the Configuration Profile from step 3
- Optionally configure certificate actions

*** Configuration Profile:**
Aruba University Secure
Select the configuration profile that will be provisioned to devices.

*** Maximum Devices:**
0
The maximum number of devices that a user may provision. Use 0 for unlimited.

Identity
These options control the generation of device credentials.

*** Certificate Authority:**
Fiermonti Onboarding CA
Select the certificate authority that will be used to sign profiles and messages.

*** Signer:**
Onboard Certificate Authority
Select the source that will be used to sign TLS client certificates.

*** TLS Certificate Authority:**
Fiermonti Onboarding CA
Select the certificate authority that will be used to sign TLS client certificates.

*** Key Type:**
2048-bit RSA - created by device
Select the type of private key to use for TLS certificates.

*** Unique Device Credentials:**
☒ Include the username in unique device credentials
When checked, the username is prefixed to the device's PEAP credentials.
This unique set of credentials is used to identify the user and device on the network.

Authorization
These options control how a device is authorized during provisioning.

*** Authorization Method:**
App Authentication — check using Aruba Application Authentication
Select the method used to authorize devices.



4. Configure Onboard Provisioning Settings

Putting it all together – General tab - Actions

- Enable email notifications for expiring certificates
- Select 1-4 weeks prior
- If email unknown, set a general mailbox
- Enter the subject line
- Customize the email by navigating to Configuration → Receipts → Templates → Certificate Expiry
- Optionally set an email address to cc or bcc

Actions
These options control actions that may be taken after device provisioning.

Certificate Expiry:
☒ Notify users before their device credentials expire
If checked users will receive an email notification when their device's network credentials are due to expire.

*** Send Email Notification:**
4 weeks prior to expiration
Select the time to send an email notification.

*** If Email is Unknown:**
Send a message to a fixed email address
Specify where to send emails to if the user's certificate doesn't have an email address recorded.

*** Unknown Address:**
onboard_expiration@arubauniversity.edu
Address used when no email address is known for a user.

Subject Line:
Your network credentials are about to expire
Enter a subject for the notification email.
Leave blank to use the default (Your network credentials are about to expire).

*** Email Message:**
Certificate Expiry
The plain text or HTML print template to use when generating an email message.

*** Email Skin:**
(Use Default: Use the default skin)
The format in which to send email receipts.

*** Send Copies:**
Always send using 'Bcc:'
Specify when to send to the recipients in the Copies To list.

Copies To:
onboard_expiration@arubauniversity.edu
An optional list of email addresses to which copies of expiry notifications will be sent.

4. Configure Onboard Provisioning Settings

Putting it all together – Supported Devices tab

- Select the devices available to be onboarded
- Under iOS and iPadOS, recommend enabling forcing the use of Safari to provide the best user experience
- Recommend setting the device detection to “Always” to allow users to select their device type should browser detection fail

Override Device Type Detection

These options control whether users can manually override the detected type of their device.

* Detection Override:

Always

If enabled, users will be able to choose their device type from a drop down.

iOS **iOS Provisioning**

These options control iOS device provisioning.

* iOS Devices:

☒ Enable iOS device provisioning

Provision iOS devices via Apple's 'Over-the-Air' profile delivery process.

iOS Browser Check:

☒ Enable browser checking for iOS

Force iOS users to provision using the default (ie Safari) browser.

iPadOS **iPadOS Provisioning**

These options control iPadOS device provisioning.

* iPadOS Devices:

☒ Enable iPadOS device provisioning

Provision iPadOS devices via Apple's 'Over-the-Air' profile delivery process.

iPadOS Browser Check:

☒ Enable browser checking for iPadOS

Force iPadOS users to provision using the default (ie Safari) browser.

4. Configure Onboard Provisioning Settings

Putting it all together – Web Login tab

- Set the page name. This is the URL that will be given to users or used in a captive portal
 - `https://<ClearPass FQDN/onboard/pagename.php`
- Customize look and feel of the login page
 - edit the title, HTML, apply a skin

Username Label:

The form label for the username field.
Leave blank to use the default (Username:).

Password Label:

The form label for the password field.
Leave blank to use the default (Password:).

Terms:

☒ Require a Terms and Conditions confirmation
If checked, the user will be forced to accept a Terms and Conditions checkbox.

Web Login Page

Options for the weblogin landing page for Onboard.

*** Page Name:**

Enter a page name for this web login.
The web login will be accessible from "/onboard/page_name.php".

*** Skin:**

Choose the skin to use when this web login page is displayed.

Title:

The title to display on the web login page.
Leave blank to use the default (Register Your Device).

Header HTML:

```
{nwa_icontext type=info}
{nwa_text id=16344}In order to connect to this network, your
device must be registered with Aruba University ITS. This wizard
will guide you through the configuration process.{/nwa_text}
{/nwa_icontext}

{capture assign=organization_name}{nwa_mdps_config
name=organization_name}{/capture}
{nwa_text id=14462 1=$organization_name|escape}Login below
using your RC credentials {/nwa_text}
```



4. Configure Onboard Provisioning Settings

Putting it all together – Web Login tab

- See below color coding for config to UX mappings based on MacOS

Header HTML:

```
{nwa_icontext type=info}
{nwa_text id=16344}In order to connect to this network, your
device must be registered with Aruba University ITS. This wizard
will guide you through the configuration process.{/nwa_text}
{/nwa_icontext}
```

```
{capture assign=organization_name}{nwa_mdps_config
name=organization_name}{/capture}
{nwa_text id=14462 1=$organization_name{escape}}Login below
using your student credentials.{/nwa_text}
```

Footer HTML:

```
{nwa_text id=7979}<p>
Contact an ITS Helpdesk member if you are experiencing
difficulty logging in.
</p>{/nwa_text}
```

Custom Labels:

☒ Override the default labels and error messages
If selected, you will be able to alter labels and error messages for the current login form.

Username Label:

Student Email Address

The form label for the username field.
Leave blank to use the default (Username:).

OS Specific messages - configured in **Pre-Login** section on the Instructions and Messages tab

macOS Instructions

These options control messages shown during macOS device provisioning.

* Pre-Login:

Use custom message

Instructions shown to the user before they log in using an macOS device.

Pre-Login Message:

For your Apple Mac, Aruba University network provisioning is a multi-step process. In order to configure your device you must follow this process to completion.

aruba
NETWORKS

Galleria Wi-Fi

In order to connect to this network, your device must be registered with Aruba University ITS. This wizard will guide you through the configuration process.

Login below using your student credentials. For your Apple Mac, Aruba University network provisioning is a multi-step process. In order to configure your device you must follow this process to completion.

Student Email Address

Password

Log In

Terms:
☐ I accept the terms of use

Contact an ITS Helpdesk member if you are experiencing difficulty logging in.

Your device was detected as a macOS device. If this is incorrect, select from this list: macOS

© Copyright 2022

4. Configure Onboard Provisioning Settings

Putting it all together – Instructions and Messages tab

- Use this tab to create customized and detailed messaging and instructions throughout the onboarding process
- Create custom messages for denied, expired, reprovisioned, or unsupported devices
- Override default messages for specific OSs
 - Android
 - iOS
 - iPadOS
 - MacOS
 - Windows
 - Web-based

Device Status
Messages related to the status of the user's device.

- Denied Device:**
Use default message
Error shown to a user when their device has been denied access.
- Expired Device:**
Use default message
Message shown to a user when their device credentials have expired. This message is displayed above the normal login page.
- Override Device Detection:**
Use default message
Message that allows the user to override the detected device type.
- Reprovision Device:**
Use default message
Message shown to a user when their device has already been enrolled.
- Unsupported Browser:**
Use default message
Error shown to the user if they attempt to provision using an unsupported browser.
- Unsupported Device:**
Use default message
Error shown to the user if they attempt to provision an unsupported device.

iPad OS iPadOS Instructions
These options control messages shown during iPadOS device provisioning.

- Pre-Login:**
Use default message
Instructions shown to the user before they log in using an iPadOS device.
- Root Certificate Download:**
Use default message
Instructions shown to the user when asked to download the iPadOS root certificate.
- Profile Download:**
Use default message
Instructions shown to the user when asked to download the iPadOS profile.
- Installing Profile:**
Use default message
Instructions shown to the user while the iPadOS profile installs.
- Complete:**
Use default message
Instructions shown to the user when iPadOS provisioning is complete.
- Link Text:**
Use default labels
Controls the labels shown on download links during iPadOS provisioning.



4. Configure Onboard Provisioning Settings

Putting it all together – Instructions and Messages tab

- Use this tab to create customized and detailed messaging and instructions throughout the onboarding process
- See below for color coded config to UX mappings based on MacOS
- *Profile Download Page* - This is the **FIRST** page post login

Message for
ALL OS
types
(will be displayed at
the top of all post-
login pages)

*** Provisioning Device:**

Use custom message ▾

Message shown to the user during the provisioning process (after login).

Provisioning Message:

```
{nwa_icontext type=info}  
{nwa_text id=16344}In order to connect to this network, your  
device must be registered with ITS. This wizard will guide you  
through the configuration process. Remember to complete all  
steps! {/nwa_text}
```

Message for
SPECIFIC OSs
(based on browser
detection or user
specified from
dropdown list)

*** Profile Download:**

Use custom message ▾

Instructions shown to the user when asked to download the macOS profile.

Profile Download Message:

```
<p><p>  
{nwa_text id=16443}For your Apple Mac, Aruba University  
network provisioning is a multi-step process. In order to configure  
your device you must download and install this provisioning profile  
which will configure your device to connect to the network.
```



4. Configure Onboard Provisioning Settings

Putting it all together – Instructions and Messages tab

- Use this tab to create customized and detailed messaging and instructions throughout the onboarding process
- See below for color coded config to UX mappings based on MacOS
- *Installing Profile page* - This is the **SECOND** page post login

Message for
ALL OS
types
(will be displayed at
the top of all post-
login pages)

*** Provisioning Device:**

Use custom message ▾

Message shown to the user during the provisioning process (after login).

Provisioning Message:

```
{nwa_icontext type=info}
{nwa_text id=16344}In order to connect to this network, your
device must be registered with ITS. This wizard will guide you
through the configuration process. Remember to complete all
steps!{/nwa_text}
```

Message for
SPECIFIC OSs
(based on browser
detection or user
specified from
dropdown list)

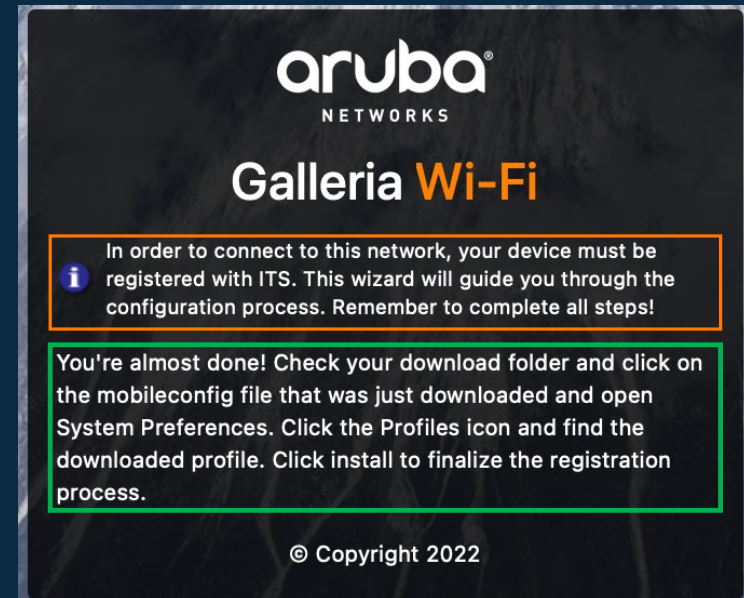
*** Installing Profile:**

Use custom message ▾

Instructions shown to the user while the macOS profile installs.

Installing Profile Message:

```
<p>
{nwa_text id=16442}You're almost done! Check your download
folder and click on the mobileconfig file that was just downloaded
and open System Preferences. Click the Profiles icon and find the
downloaded profile. Click install to finalize the registration process.
{/nwa_text}
</p>
```



4. Configure Onboard Provisioning Settings

Putting it all together – Instructions and Messages tab

- Use this tab to create customized and detailed messaging and instructions throughout the onboarding process
- See below for color coded config to UX mappings based on MacOS
- *Complete page* - This is the **FINAL** page post login

Message for
SPECIFIC OSs
(based on browser
detection or user
specified from
dropdown list)

*** Complete:**

Use custom message ▾

Instructions shown to the user when macOS provisioning is complete.

Complete Message:

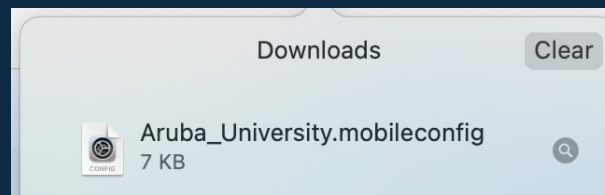
Yay! You made it! Your ever to excel spirit has rewarded you with a seamless network experience across the campus! Congratulations and Go Orange!!!



4. Configure Onboard Provisioning Settings

Putting it all together – Apple Profiles tab

- Apple devices use SCEP to enroll and install certificates
- The configuration profiles are downloaded and installed by the user
 - The Organization name from the General tab is used to name the downloaded .mobileconfig file
- Use a publicly signed cert as the profile signing cert!
 - Avoids the root certificate step
 - Marks the profile as “**verified**”



iOS, iPadOS & macOS Provisioning

These options control Apple iOS (iPod, iPhone), iPadOS and macOS (Lion or later) device provisioning.

Display Name:

Aruba University Device Enrollment

Example: 'Device Enrollment'.
This text is displayed as the title of the 'Install Profile' screen on the device.
Leave blank to use the default (Device Enrollment).

Profile Description:

This configuration profile has network and security settings for your device to allow you to connect to the Aruba Secure network.

Enter the description to display on the 'Install Profile' screen of the device.
This should provide help text for the user and instruct them to install the profile.
Leave blank to use the default (This configuration profile has network and security settings for your device to allow you to connect to the Aruba Secure network).

*** Profile Security:**

Always allow removal

Select when the configuration profile may be removed.

Edit ID:

☐ Change the profile ID

The current profile ID is 'com.example.device.provisioning.29015084-4bcf-4f02-a6c0-36d25ae44970'

Profile Signing

These options control the way profiles are signed for iOS, iPadOS and macOS devices.

*** Certificate Source:**

Use an uploaded certificate

Choose how to obtain the certificate used to sign iOS, iPadOS and macOS 10.7+ profiles.

*** Certificate:**

clearpass.fiermonti.net

Choose the code signing certificate used to sign iOS, iPadOS and macOS 10.7+ profiles.

4. Configure Onboard Provisioning Settings

Putting it all together – Apple Profiles tab

- See below for color coded config to UX mappings based on MacOS

iOS, iPadOS & macOS Provisioning
These options control Apple iOS (iPod, iPhone), iPadOS and macOS (Lion or later) device provisioning.

Display Name:
Aruba University Device Enrollment

Example: 'Device Enrollment!'
This text is displayed as the title of the 'Install Profile' screen on the device.
Leave blank to use the default (Device Enrollment).

Profile Description:
This configuration profile has network and security settings for your device to allow you to connect to the Aruba Secure network.

Enter the description to display on the 'Install Profile' screen of the device.
This should provide help text for the user and instruct them to install the profile.
Leave blank to use the default (This configuration profile has network and security settings for your device to allow you to connect to the Aruba Secure network).

*** Profile Security:**
Always allow removal
Select when the configuration profile may be removed.

Edit ID:
☐ Change the profile ID
The current profile ID is 'com.example.device.provisioning.29015084-4bcf-4f02-86c0-36d25ae41870'

Profile Signing
These options control the way profiles are signed for iOS, iPadOS and macOS devices.

*** Certificate Source:**
Use an uploaded certificate
Choose how to obtain the certificate used to sign iOS, iPadOS and macOS 10.7+ profiles.

*** Certificate:**
clearpass.fiermonti.net
Choose the code signing certificate used to sign iOS, iPadOS and macOS 10.7+ profiles.

Publicly signed certificate!



Profile settings in MacOS System Preferences

Aruba University Device Enrollment Aruba University **Verified** Ignore Install...

Description This configuration profile has network and security settings for your device to allow you to connect to the Aruba Secure network.

Signed clearpass.fiermonti.net
Received Jan 31, 2022 at 9:42 AM

Settings Profile Service Enrollment
clearpass.fiermonti.net

DETAILS

Profile Service Enrollment

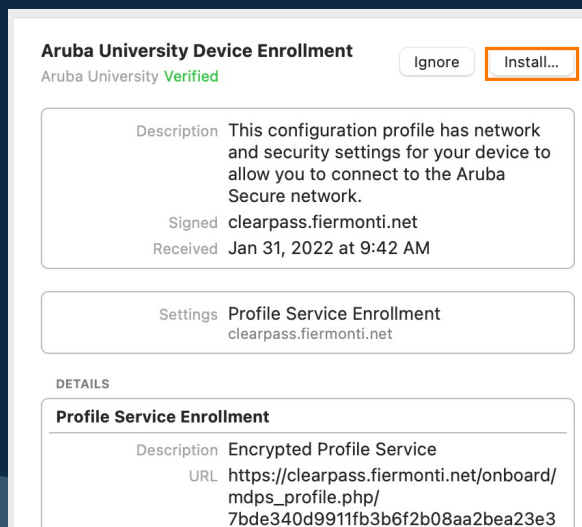
Description Encrypted Profile Service
URL https://clearpass.fiermonti.net/onboard/mdps_profile.php/7bde340d9911fb3b6f2b08aa2bea23e3

4. Configure Onboard Provisioning Settings

Putting it all together – Apple Profiles tab

- What happens when you install the profile (MacOS)

Install the profile

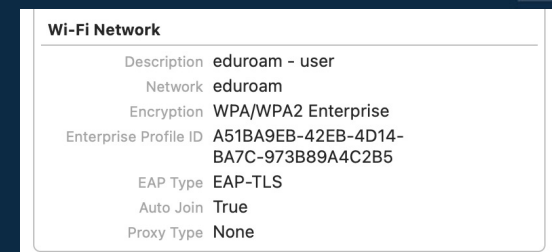
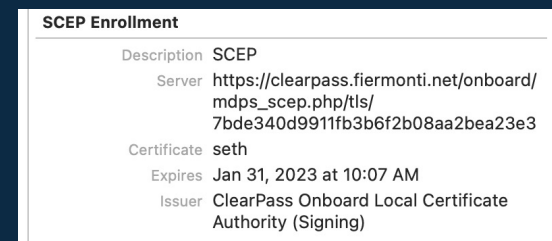
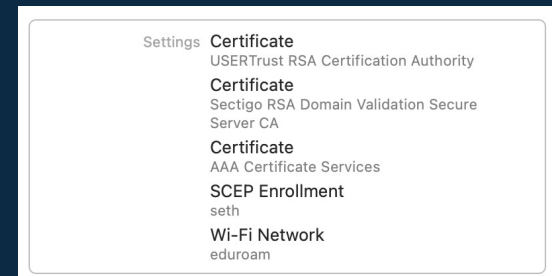


Trusted server
certs
+
Personalized TLS
cert
+
Network Settings

SCEP Process
NOTE: Certificate
Authority configured
in step 1

Wi-Fi
Network Settings
Note: EAP-TLS as
EAP type

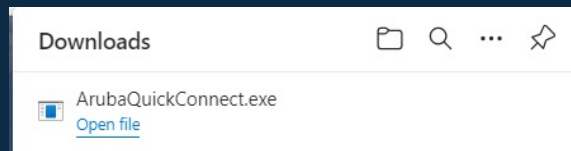
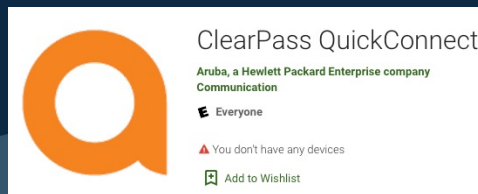
Result



4. Configure Onboard Provisioning Settings

Putting it all together – Onboard Client tab

- Used for Windows and Android onboarding
 - via ArubaQuickConnect.exe for Windows
 - via ClearPass QuickConnect app in Google Play
- Customized logo displayed in the app
 - Upload files to Configuration → Content Manager → Public Files
- Set a provisioning address
- Configure a title, password recovery and/or helpdesk URL



Device Provisioning
Options for Windows, Android and Legacy OS X (10.5/6) device provisioning. These settings are not used for iOS, iPadOS or macOS 10.7+ (Lion or later) devices.

*** Code-Signing Certificate:**
None — Use Aruba factory signature
Select a code signing certificate for signing the Windows provisioning application.

*** Provisioning Address:**
clearpass.fiermonti.net (requires DNS resolution)
Select the hostname or IP address to use for device provisioning.

Provisioning Access:
To be provisioned, devices **must** be able to access **clearpass.fiermonti.net** via **HTTPS**.

*** Validate Certificate:**
No, do not validate this web server's certificate
Specify whether the web server's certificate is to be validated during device provisioning. When testing with the default self-signed web server certificate, you may need to disable validation. This option applies to Windows, Android, and OS X 10.5/6 devices only.

Bypass Proxy:
☐ Bypass proxy server
If checked, the proxy server configured on the client will not be used during the Onboard enrollment process.

Logo Image:
Select an image to use in the provisioning wizard. New images can be uploaded using the Content Manager.

*** Wizard Title:**
Aruba University Device Enrollment Wizard
Enter a title for the wizard used on Windows and Legacy OS X (10.5/6) devices.

Password Recovery URL:
Enter the URL displayed to users who have forgotten their password.

Helpdesk URL:
https://www.arubauniversity.edu/content/it-web/offices/its/support.
Enter the URL displayed to users who require helpdesk assistance.

4. Configure Onboard Provisioning Settings

Putting it all together – Onboard Client tab

Device Provisioning
Options for Windows, Android and Legacy OS X (10.5/6) device provisioning. These settings are not used for iOS, iPadOS or macOS 10.7+ (Lion or later) devices.



*** Code-Signing Certificate:**
None — Use Aruba factory signature
Select a code signing certificate for signing the Windows provisioning application.

*** Provisioning Address:**
clearpass.fiermonti.net (requires DNS resolution)
Select the hostname or IP address to use for device provisioning.

Provisioning Access:
To be provisioned, devices must be able to access clearpass.fiermonti.net via HTTPS.

*** Validate Certificate:**
No, do not validate this web server's certificate
Specify whether the web server's certificate is to be validated during device provisioning. When testing with the default self-signed web server certificate, you may need to disable validation. This option applies to Windows, Android, and OS X 10.5/6 devices only.

Bypass Proxy:
☐ Bypass proxy server
If checked, the proxy server configured on the client will not be used during the Onboard enrollment process.

Logo Image:
 (Default) (188 x 53)

Select an image to use in the provisioning wizard. New images can be uploaded using the Content Manager.

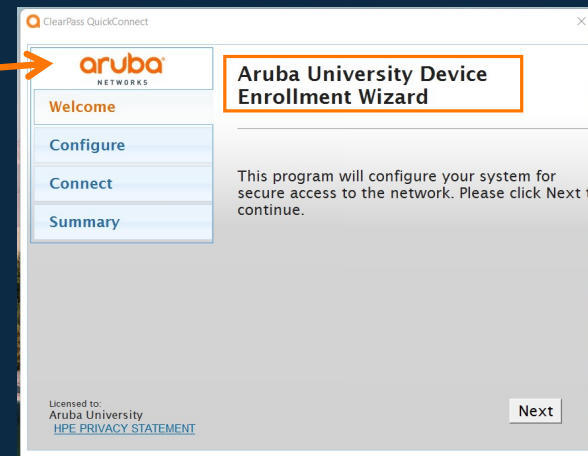
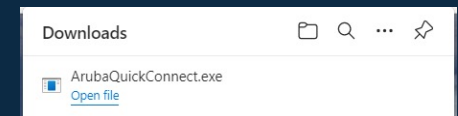
*** Wizard Title:**
Aruba University Device Enrollment Wizard
Enter a title for the wizard used on Windows and Legacy OS X (10.5/6) devices.

Password Recovery URL:

Enter the URL displayed to users who have forgotten their password.

Helpdesk URL:

Enter the URL displayed to users who require helpdesk assistance.



Optional Onboard Provisioning

Shared Computers

- Focus on Windows and MacOS
 - Restrict to these OS types
- Create a different provisioning page
- Use a shared resource identity account
 - This will become the username on the network
 - sciencelab@arubauniversity.edu
 - it_testing@arubauniversity.edu
- Create policy to only allow the shared resource accounts to onboard a device
- Use Machine certificate store in Windows
 - Configured in Onboard Network Settings
- Use System store for MacOS
 - Configured in Onboard Provisioning Settings

Use this form to make changes to the network settings that will be sent to a provisioned device. [Help](#)

Network Settings » Enterprise Authentication

Enterprise Authentication
Options for 802.1X authentication used on the network.

Android Authentication

*** Certificate Store:**
Private
Select the certificate store where the client certificate will be provisioned when configuring an Android device. Installing to the system store will make certificates available for use by other applications, but may require additional security prompts during provisioning.

iOS & macOS Authentication

*** iOS & macOS Credentials:**
Certificate
Select the type of credentials to provision for iOS and macOS 10.7+ (Lion or later) devices.

Windows Authentication

*** Certificate Store:**
Machine
Select the certificate store where the client certificate will be provisioned when configuring a Windows device.

Device Provisioning Settings

Android Provisioning
These options control Android device provisioning.

*** Android Devices:**
☐ Enable Android device provisioning
Downloads and executes an Android application on a user's device to complete provisioning.

Chrome OS Provisioning
These options control Chrome OS device provisioning.

*** Chrome OS Devices:**
☐ Enable Chrome OS device provisioning
Provides a certificate to Chrome OS devices. Requires the device to be under management and the QuickConnect.

iOS Provisioning
These options control iOS device provisioning.

*** iOS Devices:**
☐ Enable iOS device provisioning
Provision iOS devices via Apple's 'Over-the-Air' profile delivery process.

iPadOS Provisioning
These options control iPadOS device provisioning.

*** iPadOS Devices:**
☐ Enable iPadOS device provisioning
Provision iPadOS devices via Apple's 'Over-the-Air' profile delivery process.

macOS Provisioning
These options control macOS device provisioning.

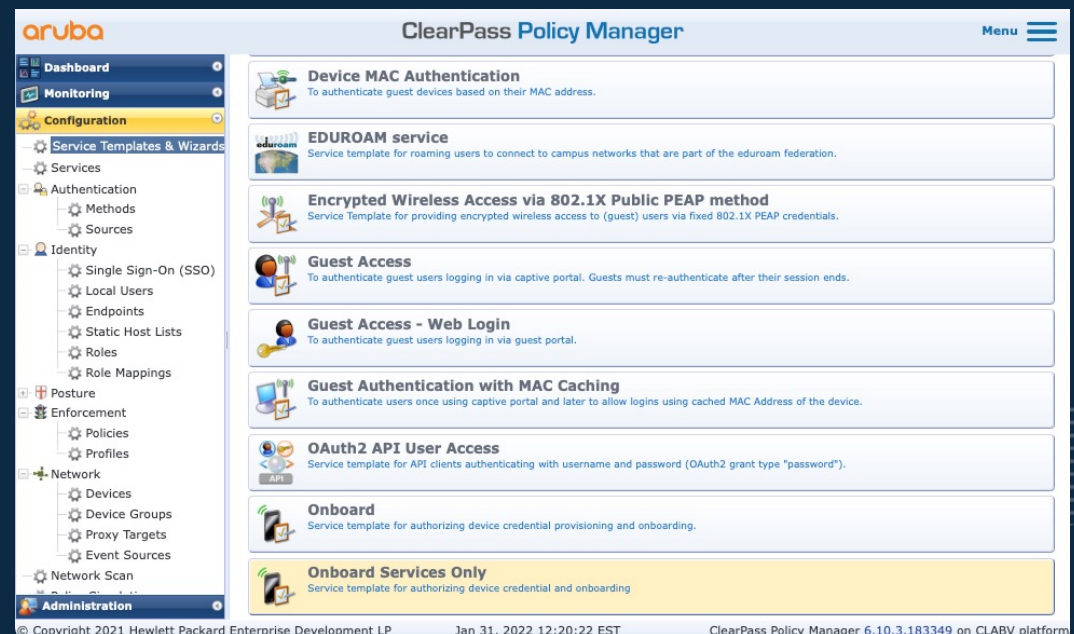
*** macOS Devices:**
☒ Enable macOS 10.7+ (Lion or later) device provisioning
Provision macOS 10.7+ (Lion or later) devices via Apple's 'Over-the-Air' profile delivery process.

Profile Type:
System
Select the type of profile to create when provisioning macOS 10.7+ (Lion or later) devices.

Onboard Services in Policy Manager

Use Wizard to setup the two services

- Navigate to Configuration → Service Templates & Wizards
 - Bottom of the list
- Select “Onboard Services Only”
- Creates two services
 1. A pre-auth service used at the web login page
 2. Authorization service used when generating and enrolling the certificate



<input type="checkbox"/>	34	Secure-Wifi Onboard Authorization	Application	Aruba Application Authorization	0
<input type="checkbox"/>	35	Secure-Wifi Onboard Pre-Auth	Application	Aruba Application Authentication	0



Onboard Services in Policy Manager

Configure the Onboard Pre-Auth and Authorization services

- Add a line to service rule to granularly apply policy to a specific onboard web login page
- Page-Name equals the web login page name configured in the Onboard provisioning settings

Configuration » Services » Edit - Secure-Wifi Onboard Pre-Auth

Services - Secure-Wifi Onboard Pre-Auth

Summary Service Authentication Roles Enforcement

Name: Secure-Wifi Onboard Pre-Auth

Description:

Type: Aruba Application Authentication

Status: Enabled

Monitor Mode: ☐ Enable to monitor network access without enforcement

More Options: ☐ Authorization

Service Rule

Matches ☐ ANY or ☒ ALL of the following conditions:

Type	Name	Operator	Value
1. Application	Name	EQUALS	Onboard
2. Application:ClearPass	Device-Name	NOT_EXISTS	
3. Application:ClearPass	Page-Name	EQUALS	device_enrollment
4. Click to add...			

- Edit the services post wizard to add AD as an authentication source

aruba ClearPass Policy Manager

Configuration » Services » Edit - Secure-Wifi Onboard Pre-Auth

Services - Secure-Wifi Onboard Pre-Auth

Summary Service Authentication Roles Enforcement

Authentication Sources:

Name	Operator	Value
Fiermonti.net AD Server - Win2016 [Active Directory]		
FiermontiHome.com AD server - Win2019 [Active Directory]		

Move Up ↑ Move Down ↓ Remove View Details Modify

Add New Authentication Source

Strip Username Rules: ☐ Enable to specify a comma-separated list of rules to strip username prefixes or suffixes



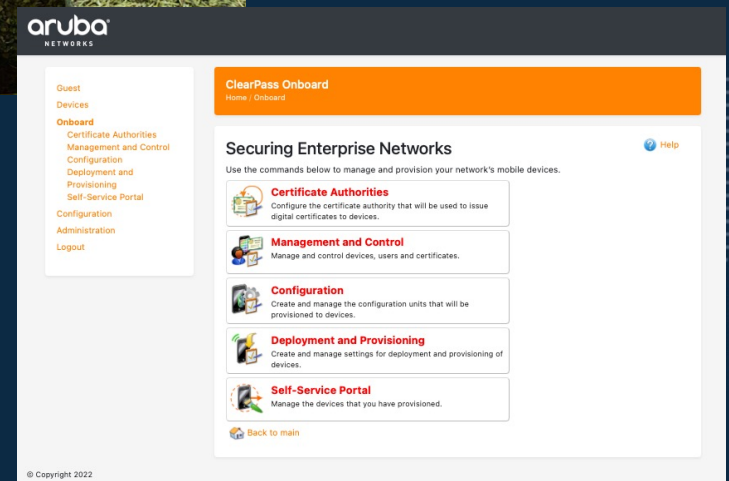
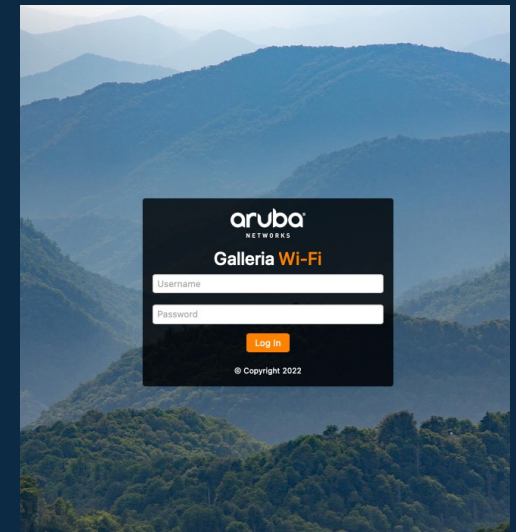
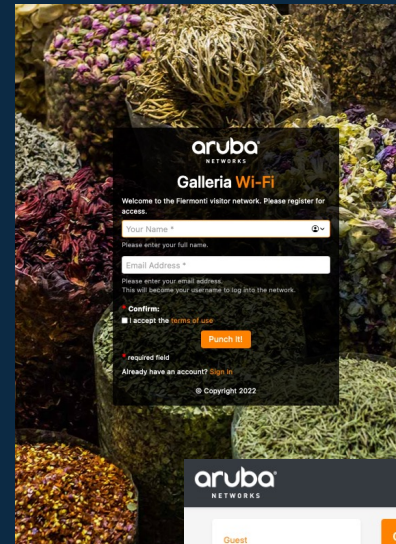
Customizing the Web Pages

How to brand and create a
familiar UX for users

BONUS: Editing the Galleria Skin

What is the Galleria Skin?

- Every installation of ClearPass includes 2 Galleria Skins.
- Easy to customize modern and professional looking web designs
- Can be applied to both user facing and administrative back end pages
- Advanced editing of HTML and CSS possible
- Turnkey service provided with Aruba Skin service



BONUS: Editing the Galleria Skin

Edit Options – Colors

- See how color options relate to web pages
- See if organization has a style or branding guide

Galleria Skin 2 6.10.3-183349 Configuration
Home / Administration / Plugin Manager

Set the configuration options for Galleria Skin 2 6.10.3-183349. [Help](#)

Configure Galleria Skin 2 6.10.3-183349

• **Version:**
Version 2 (2019 - Recommended)
Select the Galleria version to use.

• **User Scalable:**
No
Allow User Scalable in mobile layouts. For more information:
https://developer.mozilla.org/en-US/docs/Mozilla/Mobile/Viewport_meta_tag

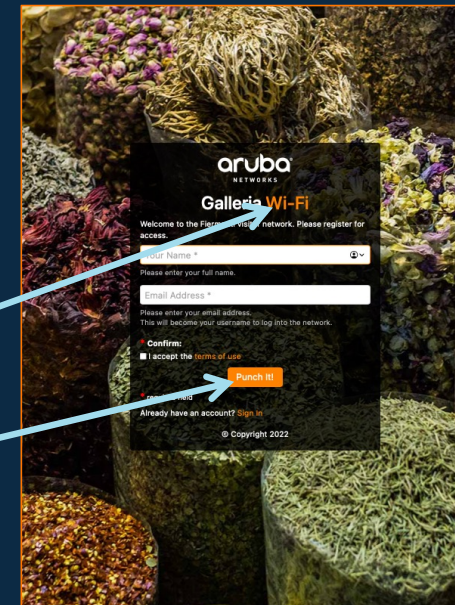
• **Theme Accent Color:**
FF8300
Select the color to be used as an accent.

• **Theme Accent Font Color:**
FFFFFF
Select the color to be used for fonts with the accent colors.

• **Theme Highlight Color:**
FF0000
Select the color to be used for highlighting important items.

Admin Display Configuration
Admin display configuration options.

• **Nav Background Color:**
343A40
Select the color to be used as the navbar background color.



aruba NETWORKS

Guest
Devices
Onboard
Certificate Authorities
Management and Control
Configuration
Deployment and Provisioning
Self-Service Portal
Configuration
Administration
Logout

ClearPass Onboard
Home / Onboard

Securing Enterprise Networks [Help](#)

Use the commands below to manage and provision your network's mobile devices.

- Certificate Authorities**
Configure the certificate authority that will be used to issue digital certificates to devices.
- Management and Control**
Manage and control devices, users and certificates.
- Configuration**
Create and manage the configuration units that will be provisioned to devices.
- Deployment and Provisioning**
Create and manage settings for deployment and provisioning of devices.
- Self-Service Portal**
Manage the devices that you have provisioned.

[Back to main](#)

© Copyright 2022



BONUS: Editing the Galleria Skin

Edit Options – Title, Logo, Icons, Copyright
– See how options relate to web pages

Title Prefix:

Galleria Wi-Fi

The prefix for the browser page title. For example: <title>...</title>

Favicon:

(default)

Select the favicon to use.

Logo:

logo-public.png (436 x 100)

The logo image to use for the skin.
Recommended: Use a high-resolution image.

Copyright:

© Copyright {"Y"}[date]

Insert...

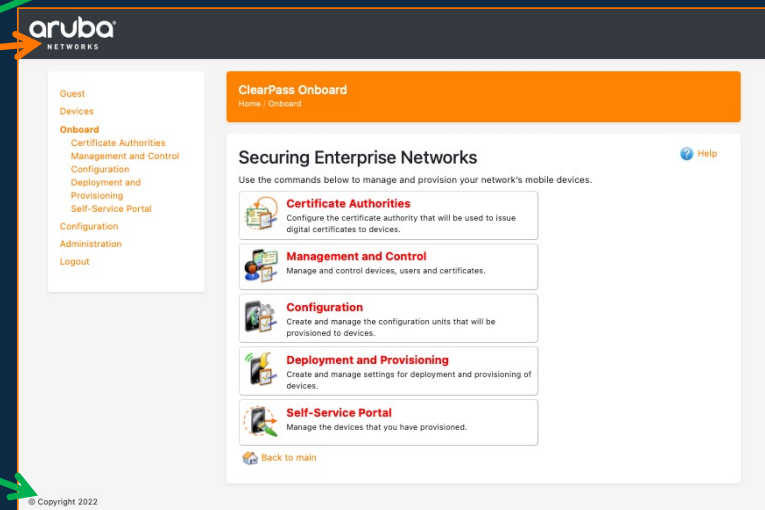
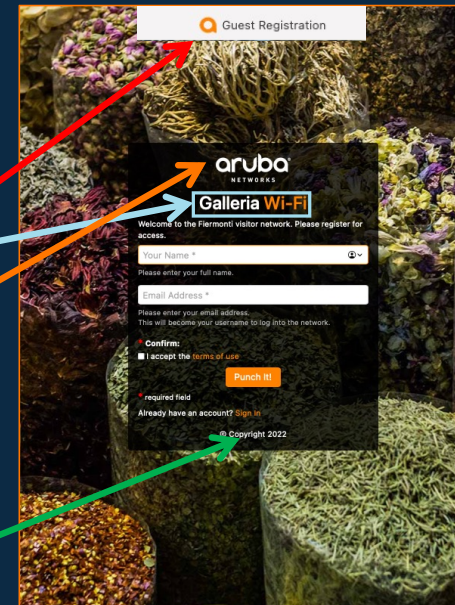
Override the copyright text for the footer.

Include Logo on Guest Login:

☒ Show Logo
Include the logo on guest-facing pages.

Include Copyright on Guest Login:

☒ Show Copyright
Include the copyright information on guest-facing pages.



BONUS: Editing the Galleria Skin

Edit Options – Background Images

- By default, the Galleria skin includes 6 images taken by Aruba employees
- Images can be edited and replaced
- Upload images to Configuration → Content Manager → Public
- Recommend creating a folder to upload images
- Larger file sizes can create a delay in rendering
- Set path in the Background Images text box
 - Path example
“/guest/public/<foldername>/<imagename>”
- Optionally set a transition delay

Guest Background Configuration
Guest-facing background and display configuration options.

*** Guest Background Mode:**
Photo Background
Select the guest-facing background mode. This will only be visible on guest-facing pages. All other pages use a flat background color.

*** Background Images:**

```
external/galleria/slideshow/v2/1_saadi.jpg
external/galleria/slideshow/v2/2_bob.jpg
external/galleria/slideshow/v2/3_stephen.jpg
external/galleria/slideshow/v2/4_landry.jpg
external/galleria/slideshow/v2/5_saadi.jpg
external/galleria/slideshow/v2/6_landry.jpg
```

Specify a list of images to use as the backgrounds. Each image should be on a separate line without commas or quotation marks.

// An Aruba "Skins Team" Production
// Photo credits: Stephen Choate + Bob Filer + Saadi Kawkji + Michael Landry
// Special thanks: Josh, Garth, and Dave
// Send comments/questions/beers to: skins@hpe.com 🍺

*** Transition Delay:**
3000
Enter the background photo transition delay time (in milliseconds).
The default is 3000ms.

BONUS: Editing the Galleria Skin

Edit Options – Guest form display

- Boxed vs Floating
- Light vs Dark (only available with Boxed option)
- Labels vs Placeholders

Boxed +
Light +
Placeholders

Boxed +
Dark +
Placeholders

Floating +
Placeholders

Boxed +
Dark +
Labels

Guest Display Customization:

Additional guest-facing customizations

• Guest Display Mode:

Boxed

Select the guest-facing display mode:

When "Boxed" mode is selected, the guest forms will be contained in a partially transparent box (this aids in readability of content).
When "Floating" mode is selected, the guest forms will be contained in a fully transparent box.

• Box Display Style:

Light

Select the box display style to use.

• Use Labels or Placeholders:

Use Placeholders

Controls if internal placeholders should be used instead of labels placed above the forms.

The form is titled "aruba NETWORKS Galleria Wi-Fi". It contains a message about connecting to the network, followed by login instructions for Apple Mac. The form has two input fields: "Student Email Address" and "Password used for Q365". Below these is a "Terms" section with a checkbox for "I accept the terms of use" and a "Log In" button. At the bottom, there is a link to contact an ITS Helpdesk member and a message about the detected device (macOS) with a dropdown menu to select the correct device.

The form is titled "aruba NETWORKS Galleria Wi-Fi". It contains a message about connecting to the network, followed by login instructions for Apple Mac. The form has two input fields: "Student Email Address" and "Password used for Q365". Below these is a "Terms" section with a checkbox for "I accept the terms of use" and a "Log In" button. At the bottom, there is a link to contact an ITS Helpdesk member and a message about the detected device (macOS) with a dropdown menu to select the correct device.

The form is titled "aruba NETWORKS Galleria Wi-Fi". It contains a message about connecting to the network, followed by login instructions for Apple Mac. The form has two input fields: "Student Email Address" and "Password used for Q365". Below these is a "Terms" section with a checkbox for "I accept the terms of use" and a "Log In" button. At the bottom, there is a link to contact an ITS Helpdesk member and a message about the detected device (macOS) with a dropdown menu to select the correct device.

The form is titled "aruba NETWORKS Galleria Wi-Fi". It contains a message about connecting to the network, followed by login instructions for Apple Mac. The form has two input fields: "Student Email Address" and "Password used for Q365". Below these is a "Terms" section with a checkbox for "I accept the terms of use" and a "Log In" button. At the bottom, there is a link to contact an ITS Helpdesk member and a message about the detected device (macOS) with a dropdown menu to select the correct device.





Advanced Onboard Policies

Use identity to change Onboard
workflows and settings

BONUS: AD Based Onboard Policies

Customize ClearPass Policy Manager Services

- As mentioned previously, there are 2 ClearPass services created for Onboard - pre-auth and authorization
- The sample request shown shows some of the details ClearPass knows about a user requesting a certificate
- Using this context, we can change onboard policies and certificates
- Following workflow will create this policy
 - New student device == 4 year certificate expiration
 - Renewed student device == 6 month certificate expiration
 - Limit students to 3 devices each

Request Details	
Summary	Input
Application:ClearPass:Device-MAC	f0:18:98: [REDACTED]
Application:ClearPass:Device-Name	Seth's MacBook Pro
Application:ClearPass:Device-Product	MacBookPro15,1
Application:ClearPass:Device-Serial	C02XR [REDACTED]
Application:ClearPass:Device-UDID	EAF704D9-FB6C- [REDACTED]
Application:ClearPass:Device-Version	20G224
Application:ClearPass:Onboard-Request-Type	New
Application:ClearPass:Page-Name	device_provisioning
Application:ClearPass:Provisioning-Settings-ID	11
Application:Name	Onboard

<input type="checkbox"/>	34	Secure-Wifi Onboard Authorization	Application
<input type="checkbox"/>	35	Secure-Wifi Onboard Pre-Auth	Application





BONUS: AD Based Onboard Policies

Edit the Certificate Authority – Increase Validity Period

- The certificate authority must have a certificate validity period greater than any value in the enforcement profile
- Set to a maximum value in days to leverage policies up to this limit
- Default value is 365 days

Certificate Issuing
These options control how certificates are issued by this certificate authority.

*** Authority Info Access:**
Do not include OCSP Responder URL 
Select the information about the certificate authority to include in the client certificate.
Note that when an OCSP URL is provided, clients may need to access this URL in order to determine if the certificate is still valid.

*** Validity Period:**
365  days
Maximum validity period for client certificates (in days).

BONUS: AD Based Onboard Policies

Create new Enforcement Profiles – Certificate Expiration using Time Source

- Profile template is “Generic Application Enforcement”
- New Onboard device will receive a 4 year certificate expiration
 - Use Session-Timeout in seconds
 - ClearPass:Session-Timeout = 126144000
- Renewed Onboard device will receive a 6 month certificate expiration
 - Use Session-Timeout in seconds
 - ClearPass:Session-Timeout = 15780000

Enforcement Profiles - Onboard Student Cert Expiration - New

Summary Profile Attributes

Profile:

Name:	Onboard Student Cert Expiration - New
Description:	
Type:	Application
Action:	Accept
Device Group List:	-

Attributes:

Attribute Name	Attribute Value
1. ClearPass:Session-Timeout	= 126144000

Enforcement Profiles - Onboard Student Cert Expiration - Renewal

Summary Profile Attributes

Profile:

Name:	Onboard Student Cert Expiration - Renewal
Description:	
Type:	Application
Action:	Accept
Device Group List:	-

Attributes:

Attribute Name	Attribute Value
1. ClearPass:Session-Timeout	= 15780000



BONUS: AD Based Onboard Policies

Create new Enforcement Profiles – max allowed devices

- Profile template is “Generic Application Enforcement”
- Create a new profile to limit Onboarded devices per user to 3

Enforcement Profiles - Onboard Student Max Devices - 3

Summary Profile Attributes

Profile:

Name:	Onboard Student Max Devices - 3
Description:	
Type:	Application
Action:	Accept
Device Group List:	-

Attributes:

	Attribute Name		Attribute Value
1.	ClearPass:Onboard-Max-Devices	=	3

BONUS: AD Based Onboard Policies

Edit the Onboard AppAuth Enforcement Policy

- Create new rules to map identity structure to the created enforcement profiles

Summary	Enforcement	Rules
Rules Evaluation Algorithm: <input type="radio"/> Select first match <input checked="" type="radio"/> Select all matches		
Enforcement Policy Rules:		
Conditions		Actions
1.	(Authorization:Fiermonti.net AD Server - Win2016:memberOf CONTAINS student) AND (Application:ClearPass:Onboard-Request-Type EQUALS New)	Onboard Student Cert Expiration - New, Onboard Student Max Devices - 3
2.	(Authorization:Fiermonti.net AD Server - Win2016:memberOf CONTAINS student) AND (Application:ClearPass:Onboard-Request-Type EQUALS Renewal)	Onboard Student Cert Expiration - Renewal, Onboard Student Max Devices - 3

BONUS: AD Based Onboard Policies

Customize the Onboard Authorization Service

- Edit the service rules
 - add the Page-Name to granularly apply policy to a specific Onboard URL
- Add identity sources as AuthZ sources
- Confirm the edited Enforcement Policy is applied to the service

Summary	Service	Authorization	Roles	Enforcement
Name:	BC User Onboard Service Authorization			
Description:	Onboard Services Only Authorization Service for Applications			
Type:	Aruba Application Authorization			
Status:	Enabled			
Monitor Mode:	<input type="checkbox"/> Enable to monitor network access without enforcement			
More Options:	<input checked="" type="checkbox"/> Authorization			
Service Rule				
Matches <input type="radio"/> ANY or <input checked="" type="radio"/> ALL of the following conditions:				
Type	Name	Operator	Value	
1. Application	Name	EQUALS	Onboard	
2. Application:ClearPass	Device-Name	EXISTS		
3. Application:ClearPass	Page-Name	EQUALS	university_onboard	

Summary	Service	Authorization	Roles	Enforcement
Strip Username Rules:	<input type="checkbox"/> Enable to specify a comma-separated list of rules to strip username prefixes or suffixes			
Authorization Details:	Additional authorization sources from which to fetch role-mapping attributes -			
	Fiermonti.net AD Server - Win2016 [Active Directory]		Remove	
	[Local User Repository] [Local SQL DB]		View Details	
			Modify	
	--Select to Add--			



Creating the Onboard Self-Service Portal

Allow users to self-manage their
own devices and certificates

BONUS: Self-Service Enablement

Portal for Onboarded device lifecycle management

- Ability for users to self-manage their own devices
- Uses Operator Profiles already pre-built in ClearPass
- Customize new Operator Profiles to suit organization's needs
- Ability to see only one's own devices, any devices shared between a common group, or administrative access for complete visibility
- Actions to mark a device lost or delete a device/user

The screenshot displays the Aruba Self-Service Portal. On the left, a sidebar contains links for 'Devices', 'Onboard', 'Self-Service Portal', and 'Logout'. The main content area is titled 'Self-Service Portal' and includes a breadcrumb trail: 'Home / Onboard / Self-Service Portal'. Below the title, a message states 'Use this list to manage your devices.' A 'Columns' section features a 'Device Type' dropdown set to 'All' and a 'Keywords' search bar with the instruction 'Filter by Product Name, Device Name, MAC Address or Device UDID.' The central part of the interface is a table with the following data:

Name	Owner	Device Type	Device Status	MAC Address
iOS Apple iPhone	student	iOS	✓ Allowed	
Seth's MacBook Pro	student	OS X	✓ Allowed	f0:18:98:...
Windows 10	student	Windows	✓ Allowed	38:87:d5:...

Below the table, there is a 'Refresh' button, a count of '1' device, and pagination information: 'Showing 1 - 3 of 3' and '20 rows per page'. At the bottom, there are links for 'Back to Onboard' and 'Back to main'. A copyright notice '© Copyright 2022' is visible in the bottom left corner of the interface.

BONUS: Self-Service Enablement

Portal for Onboarded device lifecycle management

- Controlling access to guest/onboard is done via Administration → Operator Logins → Profiles
- BYOD Operator is the pre-built profile
 - Duplicate this profile to build your own custom access like “Student”
 - Example shown to the right

The screenshot shows the 'Operator Profiles' page in the ClearPass Guest portal. The left sidebar contains a navigation menu with categories: Guest, Devices, Onboard, Configuration, Administration (highlighted), and Operator Logins. Under 'Administration', there are links for API Services, Aruba Integrations, Check Security, Data Retention, Extensions, Import Configuration, and Operator Logins. Under 'Operator Logins', there are links for Login Configuration, Profiles (highlighted), Servers, Translation Rules, Plugin Manager, Support, and Logout. The main content area is titled 'Operator Profiles' and includes a breadcrumb trail: Home / Administration / Operator Logins / Profiles. It contains explanatory text about role-based access control and a table of operator profiles. The 'BYOD Operator' profile is highlighted with a blue border. Below the table, there are links for 'Show Details', 'Edit', 'Delete', 'Duplicate', and 'Show Usage' for the selected profile.

Name	Description
API Guest Operator	Operators with this profile can use the API to manage guest accounts.
API Read Only	
BYOD Operator	Operators with this profile can view and manage their own provisioned devices.
Device Registration	Operators with this profile can self-provision their devices, for use with MAC authentication and AirGroup sharing.
Help Desk	Operators with this profile can troubleshoot problems reported by end users.
Network Administrator	Operators with this profile can view and configure network-related settings.
Null Profile	Default profile with no permissions.
Operations and Marketing	Operators with this profile can configure guest workflows, manage print templates and control other application customization options.
Read-only Administrator	Operators with this profile have read-only access to the entire system.
Receptionist	Operators with this profile are limited to creating new accounts and sending receipts only, and will see the create account form on login.

The screenshot shows the 'Onboard' permissions configuration page. It features a dropdown menu set to 'Custom...'. Below the dropdown, there is a list of permissions for managing Onboard device provisioning. Each permission has a corresponding radio button for selecting the access level: No Access, Read Only, or Full. The 'BYOD Operator' profile is selected, and its permissions are shown. The permissions are as follows:

- Configure Provisioning: ☒ No Access ☐ Read Only ☐ Full
- Create New CSR: ☒ No Access ☐ Read Only ☐ Full
- Delete Certificate: ☒ No Access ☐ Read Only ☐ Full
- Delete Own Devices: ☐ No Access ☐ Read Only ☒ Full
- Delete Shared Devices: ☐ No Access ☐ Read Only ☒ Full
- Disable Own Devices: ☐ No Access ☐ Read Only ☒ Full
- Disable Shared Devices: ☐ No Access ☐ Read Only ☒ Full
- Enable Own Devices: ☐ No Access ☐ Read Only ☒ Full
- Enable Shared Devices: ☐ No Access ☐ Read Only ☒ Full
- Export CA Private Key: ☒ No Access ☐ Read Only
- Export Private Key: ☒ No Access ☐ Read Only
- Import Code-Signing Certificate: ☒ No Access ☐ Read Only ☐ Full
- Issue Certificate: ☒ No Access ☐ Read Only ☐ Full
- Issue Subordinate CA Certificate: ☒ No Access ☐ Allow Access
- Manage Certificate Authorities: ☒ No Access ☐ Read Only ☐ Full
- Manage Devices: ☒ No Access ☐ Read Only ☐ Full
- Manage Own Devices: ☐ No Access ☐ Read Only ☒ Full
- Manage Shared Devices: ☐ No Access ☐ Read Only ☒ Full
- Revoke Certificate: ☒ No Access ☐ Read Only ☐ Full
- View Certificate: ☒ No Access ☐ Read Only
- View Own Certificate: ☐ No Access ☒ Read Only

BONUS: Self-Service Enablement

Portal for Onboarded device lifecycle management

- Map Operator Profile to Policy
- In Enforcement Profile, use the attribute “admin_privileges”
- Tie Enforcement Policy to these new Profiles

Services - Guest Operator Login to AD

Summary Service Authentication Roles **Enforcement**

Use Cached Results: ☐ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: Guest Operator Logins to AD Modify

Enforcement Policy Details

Description:	
Default Profile:	[Deny Application Access Profile]
Rules Evaluation Algorithm:	first-applicable

Conditions	Enforcement Profiles
1. (Authentication:Username EQUALS_IGNORE_CASE seth)	Guest Admin User
2. (Tips:Role EQUALS Student)	Guest Student User

Configuration » Enforcement » Profiles » Edit Enforcement Profile - Guest Student User

Enforcement Profiles - Guest Student User

Summary Profile Attributes

Profile:

Name:	Guest Student User
Description:	Enforcement profile for Guest admin logins
Type:	Application
Action:	Accept
Device Group List:	-

Attributes:

Attribute Name	Attribute Value
1. admin_privileges	= Student

Enforcement Profiles - Guest Admin User

Summary Profile Attributes

Profile:

Name:	Guest Admin User
Description:	Enforcement profile for Guest admin logins
Type:	Application
Action:	Accept
Device Group List:	-

Attributes:

Attribute Name	Attribute Value
1. admin_privileges	= Super Administrator

